IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

STINGRAY IP SOLUTIONS LLC, Plaintiff, v. SNAP ONE HOLDINGS CORP. and SNAP ONE, LLC, Defendants.	§ § § § § § § § § §	CIVIL ACTION NO. _____ JURY TRIAL DEMANDED

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Stingray IP Solutions LLC ("Stingray") files this Complaint in this Eastern District of Texas (the "District") against Defendants Snap One Holdings Corp. and Snap One, LLC (collectively, "Defendants" or "Snap One") for infringement of U.S. Patent No. 7,224,678 (the "'678 patent"), U.S. Patent No. 7,440,572 (the "'572 patent"), U.S. Patent No. 7,441,126 ("the "'126 patent"), and U.S. Patent No. 7,616,961 ("the "'961 patent").

THE PARTIES

1. Stingray IP Solutions, LLC ("Stingray" or "Plaintiff") is a Texas limited liability company, located at 6136 Frisco Sq. Blvd., Suite 400, Frisco, TX 75034.

2. On information and belief, Defendant Snap One Holdings Corp. ("Snap Holdings") is a publicly traded corporation formed and organized under the laws of Delaware with its principal executive offices and corporate headquarters located at 1800 Continental Boulevard, Suite 200, Charlotte, North Carolina. Snap Holdings' registered agent in Delaware is Intertrust Corporate Services Delaware Ltd. located at 200 Bellevue Parkway, Suite 210, Wilmington, DE 19809. Snap Holdings stock is traded in the NASDAQ Global Select (GS) stock market under the symbol "SNPO."

3. On information and belief, Defendant Snap One, LLC ("Snap LLC") is a corporation formed and organized under the laws of North Carolina with its principal place of business at 1800 Continental Blvd, Suite 200, Charlotte NC 28273-6388. Snap LLC is registered to do business in Texas and maintains Attorney Service Associates, Inc., 3610-2 N Josey Ln, Ste 223, Carrollton, TX 75007, as its registered agent in Texas. *See* TEXAS SECRETARY OF STATE, https://direct.sos.state.tx.us/ at Filing No. 801420465 (showing Snap One LLC's 2021 Public Information Report in Texas) (last visited Nov. 18, 2022). Snap One, LLC is a wholly owned subsidiary of Defendant Snap Holdings.

4. In about August of 2019, Snap AV, a "manufacturer of A/V, surveillance, networking and remote management products for professionals" and Control4 Corporation, a "global provider of smart home solutions" merged their businesses to form a single organization referred to as "Snap AV." *See SnapAV, Control4 Merger Complete*, CEPRO, https://www.cepro.com/news/snapav_control4_merger_approved/ (last visited Nov. 18, 2022). The business rebranded itself as "Snap One" in 2021. *See We're Snap One, Nice to Meet You*, SNAP ONE, https://www.snapone.com/our-story (last visited Nov. 18, 2022).

5. Snap One manufactures products that "encompass the spectrum of solutions needed to deliver integrated smart living systems" (referred to herein as the "Snap One products"). *See 2021 Snap One Annual Report*, SNAP ONE, *available for download as a pdf file at* https://investors.snapone.com/financial-information/sec-filings?items_per_page=10&page=2 (last accessed Nov. 18, 2022). The Snap One business is organized with Snap One Holdings Corporation (which is Defendant Snap Holdings in this lawsuit) as the parent and holding company of various subsidiaries, including Snap One, LLC (which is Defendant Snap LLC in this lawsuit). *See id.* at 44. Defendant Snap LLC "together with its subsidiaries, owns substantially all of [Snap Holdings']

operating assets." *Id*. Snap One also utilizes contract manufacturers and component supply vendors to produce the Snap One products. *Id*. at 26.

6. The Snap One business "enabl[es] professional integrators to deliver seamless experiences in the connected homes and small businesses where people live, work and play." *See 2021 Snap One Annual Report* at 6. Snap One utilizes an "Only Here" strategy that allows a network of "over 16,000" integrators "access a leading, comprehensive suite of products and software solutions that enable a 'one-stop shop' experience." *Id*. Snap One utilizes an "industry-leading remote management software platform, which reaches approximately 424,000 active homes and businesses. *Id*. Snap One serves integrators who are "small- to medium-sized businesses that enable smart living for their customers." *Id*. Moreover, Snap One states that these integrators are "experts at designing, installing, and servicing complex, fully integrated connected home and business systems, which include products such as audio, video, surveillance, lighting, home automation, and more for both homeowners and commercial customers." *Id*.

7. Snap One describes its Snap One products as "a leading, comprehensive suite of connected, infrastructure, entertainment, and software solutions so the entire smart living experience is exceptional for the end consumer." *See 2021 Snap One Annual Report* at 8. Snap One's line of products are offered under at least the Control4™, araknis™, Access Networks®, pakedge®, Clare™, WattBox® SunbriteTV™, and Allnet™ brands and include "a broad range of proprietary SKUs that encompass the spectrum of solutions needed to deliver integrated smart living systems…sold under [its] proprietary brands." *Id*.; *see also Solutions Designed for You*, SNAP ONE, https://www.snapone.com/solutions-brands (listing Snap One's "solutions for connected homes and businesses"). Snap One's "product portfolio extends across the Connected, Entertainment and Infrastructure product categories." *See 2021 Snap One Annual Report* at 12; *see*

also Support, SNAP ONE, https://www.snapav.com/shop/en/snapav/support (providing a link to download Snap One's product catalog) (last visited Nov. 18, 2023). Snap One's Connected Products include "networking, control and lighting surveillance and power." *See 2021 Snap One Annual Report* at 12.

8. On information and belief, Snap One has its principal executive offices in Charlotte, North Carolina, where Defendants Snap Holding and Snap LLC jointly maintain their headquarters, and in Draper, Utah. *See 2021 Snap One Annual Report* at 52. Snap One maintains "local branches across the United States and seven distribution centers located in California, Kentucky, North Carolina, Texas, Utah, the United Kingdom and Australia." *Id.* And it leases or subleases "all of [its] corporate offices, distribution centers and local branch spaces." Snap One's "material operating locations" are also located in Hebron, Kentucky, San Bernardino, California, and, highly relevant to this lawsuit, Carrollton, Texas. *Id.* Snap One has over 1,400 employees with 1,300 of those employees working in the United States. *Id.* at 16.

9. On information and belief, Snap One does business in Texas and this District via at least its operating location in Carrollton. Snap One is also registered to do business in Texas via its subsidiary Defendant Snap LLC, which has maintained its registration since 2011, originally as "Wirepath Home Systems, LLC." *See Search Results for "Snap One" as a Business Entity*, TEXAS SECRETARY OF STATE, *accessible at* https://direct.sos.state.tx.us/.

10. On information and belief, Defendants on their own and/or via subsidiaries, distributors, integrators, and affiliates maintain a corporate and commercial presence in the United States, including in Texas and this District. Defendants maintain their business presence in the U.S. and Texas via at least the following activities: 1) providing corporate, distribution, and branch locations across the U.S. (including at least one in Texas); 2) maintaining an online presence for

the sale of Snap One products (e.g., https://www.snapone.com/solutions-brands, https://www.snapav.com/shop/en/snapav, https://www.accessnetworks.com/, https:// pakedge.com/, https://www.clarecontrols.com/, https://www.control4.com/solutions/catalog, https:// araknisnetworks.com/, and https://www.allnetdistributing.com/) that solicits sales of Snap One products under at least the Control4™, araknis™, Access Networks®, pakedge®, Clare™, WattBox® SunbriteTV™, and Allnet™ brands; 3) distributing the Snap One products, via wholesale and retail channels, including via "contracts with integrators, distributors and retailers" in this District; 4) providing to U.S. consumers "a subscription service that allows end consumers to control and monitor their homes remotely and allows the end consumer's respective integrator to perform remote diagnostic services for accessing product information," and other services related to Snap One products; 5) establishing a network of 16,000 professional integrators that provide the Snap One products and/or services to 424,000 homes and businesses; and 6) employing at least 1,400 persons in the United States, including residents of Texas and this District. For example, Defendants employ Texas residents in at least one branch located at 2901 Trade Center Dr. 120, Carrollton, TX 75007. *See, e.g.*, *Give Your Career the Smart It Deserves*, SNAP ONE, https://careers-snapone.icims.com/jobs/intro (providing a link to Snap One's job search portal, which identifies where Snap One is hiring) (last visited Nov. 22, 2022). Thus, Defendants Snap Holdings and Snap LLC do business in the United States, the state of Texas, and in the Eastern District of Texas.

JURISDICTION AND VENUE

11. This action arises under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others.

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

A. Defendant Snap Holdings

13. On information and belief, Defendant Snap Holdings is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein, including its registration to do business in Texas, via its subsidiary Snap LLC, which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, affiliates, integrators, and/or consumers.

14. For example, Snap Holdings owns and/or controls multiple, subsidiaries, distributors, and affiliates including, but not limited to, Defendant Snap LLC. Snap LLC operates in the U.S. and in Texas under the name and brand "Snap One," which is the same name used by its parent Defendant Snap Holdings. Via at least its subsidiaries and partner integrators, Snap Holdings maintains a significant business presence in Texas by employing residents in at least branch/distribution locations in Carrollton, TX. *See, e.g.*, *2021 Snap One Annual Report* at 52 (listing Snap One's properties where it conducts material operations). Snap Holdings, via at least the operations of its subsidiary Snap LLC, owns or leases a branch facility in this District at 2901 Trade Center Dr. 120, Carrollton, TX 75007. *See Property Search Results > 1-1 of 1 for Year 2022*, DENTON CAD, https://propaccess.trueautomation.com/clientdb/SearchResults.aspx?cid=19 (Search results for "Snap One" as owner) (last visited Nov. 9, 2022). Importantly, Snap Holdings maintains its own employees or agents at this facility to conduct its business of at least distribution

of Snap One products. *See, e.g., Search Results of Job Listings at the "US-TX-Carrollton" location,* https://careers-snapone.icims.com/jobs/search?ss=1&searchLocation=12781-12827-Carrollton&mobile=false&width=1128&height=500&bga=true&needsRedirect=false&jan1offset=-360&jun1offset=-300 (showing a "Sales Engineer" position open for hiring at the Carrollton, TX location) (last visited Nov. 22, 2022).

15. Such a corporate and commercial presence by Defendant Snap Holdings furthers the development, design, manufacture, importation, distribution, sale, and use of Defendants' infringing electronic devices in Texas, including in this District. Through utilization of its business segments (including prior acquisitions and mergers) and the direction and control of its subsidiaries, integrators, and affiliates, Snap Holdings has committed acts of direct and/or indirect patent infringement within Texas, this District, and elsewhere in the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over Snap Holdings would not offend traditional notions of fair play and substantial justice.

16. Upon information and belief, Snap Holdings controls or otherwise directs and authorizes all activities of its subsidiaries, distributors, and affiliates, including, but not limited to Defendant Snap LLC, which, jointly have substantial business operations in Texas. Directly via or jointly in concert with at least these segments, subsidiaries, distributors, and/or affiliates and through the activities of intermediaries, such as professional integrators, resellers, dealers, expert installers, and customers, Snap Holdings has placed and continues to place infringing electronic devices, including Snap One's audio/video ("AV"), security, smart home, networking, and automation products, such as Control4™, araknis™, Access Networks®, pakedge®, Clare™, WattBox®, SunbriteTV™, and Allnet™ branded devices, into the U.S. stream of commerce. Snap Holdings has placed such products into the stream of commerce with the knowledge and

understanding that such products are, will be, and continue to be sold, offered for sale, and/or imported into this District and the State of Texas. *See Litecubes, LLC v. Northern Light Products, Inc.*, 523 F.3d 1353, 1369-70 (Fed. Cir. 2008) ("[T]he sale [for purposes of § 271] occurred at the location of the buyer."); *see also Semcon IP Inc. v. Kyocera Corporation*, No. 2:18-cv-00197-JRG, 2019 WL 1979930, at *3 (E.D. Tex. May 3, 2019) (denying accused infringer's motion to dismiss because plaintiff sufficiently plead that purchases of infringing products outside of the United States for importation into and sales to end users in the U.S. may constitute an offer to sell under § 271(a)).

17. Based on Defendant Snap Holdings' connections and relationship with its distributors, segments, subsidiaries, including its wholly owned subsidiary Snap LLC, resellers, contractors, professional integrators, dealers, installers, retailers, and digital distribution platforms, Snap Holdings knows that Texas is a termination point of the established distribution channel for the sale and use of Snap One AV, security, smart home, networking, and automation products and related software to consumers in Texas. Snap Holdings, therefore, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this basis.

18. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant Snap Holdings has committed acts of infringement in this District. As further alleged herein, Defendant Snap Holdings, via its own operations and employees located there and via ratification of Defendant Snap LLC's presence and activities, including as an agent and alter ego of Defendant Snap Holdings, has a regular and established place of business, in this District. Snap Holdings' regular and established place of business is at least located at 2901 Trade Center Dr. 120, Carrollton, TX 75007, which according to publicly available records is located in Denton County. Accordingly, Snap Holdings may be sued in this district under 28 U.S.C. § 1400(b).

B. Defendant Snap LLC

19. On information and belief, Defendant Snap LLC is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, Snap LLC has been registered to do business in Texas since 2011. Moreover, Snap LLC, including as an alter ego and agent of parent company Snap Holdings, owns and operates a branch/distribution facility where employees and/or agents of Defendants work to store, distribute, and sell Snap One products, including related services and administration of the Snap One business. This facility is located in Denton County at 2901 Trade Center Dr. 120, Carrollton, TX 75007.

20. Defendant Snap LLC further is responsible for importing, shipping, distributing, selling, offering for sale, delivering, and using Snap One's AV, security, smart home, networking, and automation products, such as Control4™, araknis™, Access Networks®, pakedge®, Clare™, WattBox®, SunbriteTV™, and Allnet™ branded devices and purposefully placing infringing Snap One products in established distribution channels in the stream of commerce in the U.S., including in Texas and this District. For example, Snap LLC, in concert with Snap Holdings distributes its products to residents of Texas and this District, via distributors, professional integrators, contractors, original equipment manufacturers, dealers, retailers, and online merchants (including

its own online stores). *See New Product Premiere*, SNAP ONE, https://www.snapav.com/shop/en/snapav/home (providing a website for Snap LLC's customers to browse Snap One's categories of products, including new products) (last visited Nov. 10, 2022). Snap LLC also maintains a physical presence via Snap One's branch/distribution center located 2901 Trade Center Dr. 120, Carrollton, TX 75007. Moreover, Snap LLC provides "Partner Stores" that provide to residents of Texas and this District "a local brick-and-mortar presence, offering more choice and access to products, hands-on training, design assistance, and in-person experts always ready to help." *See Snap One Partner Stores*, SNAP ONE, https://www.snapone.com/contact-us#partner-stores (last visited Nov. 10, 2022). Such Partner Stores are located in the State of Texas at 3007 Longhorn Blvd. #111, Austin, TX 78758; 7450 Harwin Drive, Houston, TX 77036; and 2009 McKenzie Drive #102, Carrollton TX 75006. *See Contact Us*, ALLNET DISTRIBUTING, https://www.allnetdistributing.com/ (listing these addresses as locations for its Snap One Partner Store, Allnet) (last visited Nov. 22, 2022). Snap LLC also provides "subscription services associated with product sales including hosting services, technical support, and access to unspecified software updates and upgrades." *See 2021 Snap One Annual Report* at 61. These subscription services further facilitate and allow the use of Snap One products "allow[ing] end consumers to control and monitor their homes remotely and allows the end consumer's respective integrator to perform remote diagnostic services." *Id*. at 70. Defendant Snap LLC, therefore, has purposefully directed its activities in Texas, and should reasonably anticipate being brought in this Court.

21. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant Snap LLC has committed acts of infringement in this District and has one or more regular and established places of business in this District. One such regular and

established place of business located in Denton County is the Snap LLC facility located at 2901 Trade Center Dr. 120, Carrollton, TX 75007, which Snap LLC utilizes for the Snap One business (including on behalf and for the benefit of Snap Holdings), via Snap One's employees and/or agents, to store, distribute, sell, and use Snap One products in this District, Texas, and the U.S. Accordingly, Defendant Snap LLC may be sued in this district under 28 U.S.C. § 1400(b).

22. On information and belief, Defendants Snap Holdings and Snap LLC each have significant ties to, and presence in, the State of Texas and the Eastern District of Texas, making venue in this District both proper and convenient for this action.

THE ASSERTED PATENTS AND TECHNOLOGY

23. The Asserted Patents cover various aspects of monitoring, detecting intrusions, and encrypting and decrypting wireless communications networks, including networks created between Snap One's AV, security, smart home, networking, and automation products.

24. The '678 patent involves detecting intrusions into a wireless local or metropolitan area network. The disclosed intrusion detection techniques include monitoring transmission between stations of the network, where each station has its own media access layer (MAC) address. The monitoring is done to detect failed attempts to authenticate the MAC addresses. Upon detection of a number of failed attempts to authenticate, an intrusion alert may be generated.

25. The '572 patent involves providing secure wireless local area networks (LAN). A device for securing such a LAN may include a housing with a wireless transceiver carried by the housing. A medium access controller (MAC) also carried by the housing. A cryptography circuit may be connected to the MAC controller and the transceiver. The circuit may encrypt both address and data information by at least adding a plurality of encrypting bits to be transmitted. And the cryptography circuit may decrypt both address and data information upon reception.

26. The ’126 patent provides a secure wireless local area network (LAN) utilizing a LAN device. This device may include a housing that carries a wireless transceiver and, a media access controller (MAC). A cryptography circuit carried by the housing may be connected to the MAC and the wireless transceiver. And the cryptography circuit may comprise a volatile memory provided for storing cryptography information and may also comprise a battery provided for maintaining the cryptography information stored on the volatile memory.

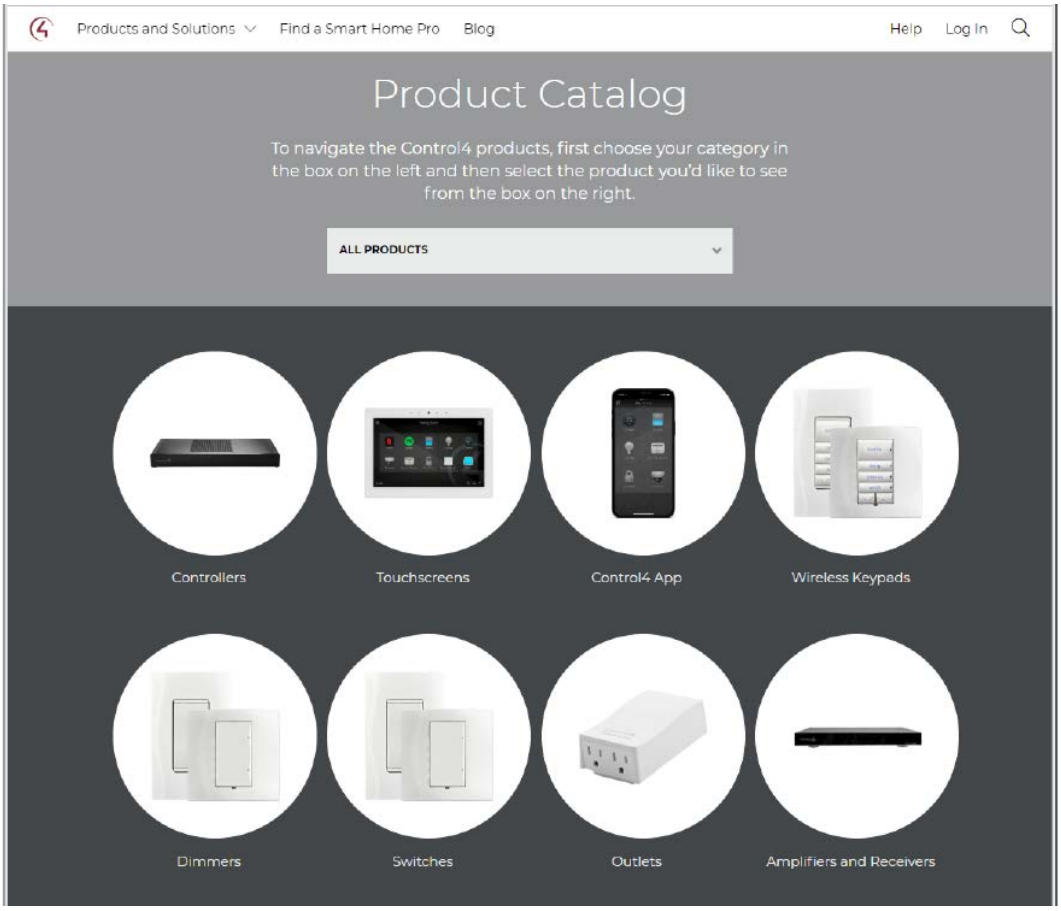
27. The ’961 patent involves allocating channels in mobile ad hoc networks. The patent describes dynamic channel allocation in such networks to efficiently make use of a plurality of channels. In such networks, wireless communication links connect wireless mobile nodes over multiple separate channels at different frequencies. The disclosed techniques for channel allocation include monitoring link performance on one channel based on a quality of service (QoS) threshold. When the monitored link performance falls below the QoS threshold, other available separate channels are scouted. Scouting may include switching to a second separate channel at a different frequency. A channel activity query may be broadcast to determine link performance of the second separate channel. Replies to the query are processed to determine the link performance, and channel activity may be updated for each separate channel based on the replies.

28. On information and belief, a significant portion of the operating revenue of Defendants is derived from the manufacture and sale of at least Snap One’s AV, security, smart home, networking, and automation products. *See 2021 Snap One Annual Report* at 61 (“We generate net sales by selling hardware products to our integrators both with and without embedded software, which are then resold to end consumers, typically in the installation of an audio/video, IT, smart-home, or surveillance-related package.”). For example, Defendant Snap Holdings and Snap LLC jointly utilize their distributors, subsidiaries, resellers, contractors, dealers, installers, retailers,

and digital distribution platforms to provide Snap One's AV, security, smart home, networking, and automation products and related services to consumers. For the year 2021, Defendants reported $1.01 billion in "Net Sales" as revenue. *See 2021 Snap One Annual Report* at 61. Moreover, "a small but growing percentage of our revenue through recurring revenue from subscription services associated with product sales including hosting services, technical support, and access to unspecified software updates and upgrades." *Id*.

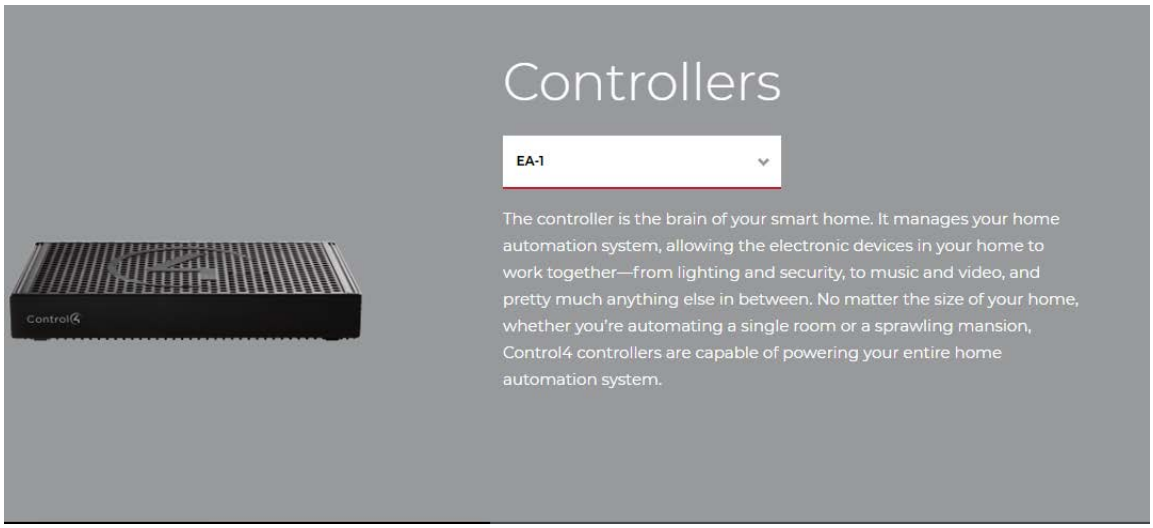
29. The Asserted Patents cover Snap One's AV, security, smart home, networking, and automation products and components, software, services, and processes related to same that generally connect to other devices in a network or other networks using a wireless protocol, such as Wi-Fi or ZigBee (collectively referred to herein as the "Accused Products"). *See Shop | Categories*, SNAP ONE, https://www.snapav.com/shop/en/snapav/home (providing purchasers a search platform to access Snap One's categories of products offered, including Snap One's own products) (last visited Nov. 15, 2022). Defendants' infringing Accused Products include, but are not limited to, devices enabled or compliant with Wi-Fi such as smart home systems, which include controllers, touch screens, remotes, routers and access points, USB adapters, cameras, surge protectors and outlets, thermostats, and audio speakers. *See, e.g., id*. (providing search results for 'wifi' products offered by Snap One and filtered to show only Snap One brands).

30. Examples of Snap One's Wi-fi enabled or compliant products include Snap One's smart home systems sold under the Control4 brand, as shown below.



Product Catalog, CONTROL4, https://www.control4.com/solutions/catalog (last accessed Nov. 15, 2022).

31. Components of Snap One's smart home systems utilize Wi-fi for network connectivity. As shown below, the Control4 EA-1 Controller utilizes Wi-fi, i.e., 801.11n/g/b, to function as "manage[] your home automation system, allowing the electronic devices in your home to work together—from lighting and security, to music and video, and pretty much anything else in between."



Controllers, CONTROL4, https://www.control4.com/solutions/products/controllers (last visited Nov. 15, 2022).

Network	
Ethernet	10/100/1000BaseT compatible (required for controller setup)
WiFi	Wireless-N (2.4 GHz, 802.11n/g/b)
WiFi security	WPA/WPA2
WiFi antenna	External reverse SMA connector
Zigbee Pro	802.15.4
Zigbee antenna	External reverse SMA connector
USB port	1 USB 2.0 port—500mA
Control	

Control4 EA-1 | Datasheet, CONTROL4, *accessible as a pdf at* https://www.control4.com/docs/product/ea-1/data-sheet/english/latest (last visited Nov. 15, 2022).

32. The Defendants' touch screens, such as the T4 Series Touch Screens shown below, allow consumers to "manage lighting, security, music, televisions, temperature, shades, and more," via a Wi-Fi connection to a wireless network.

Control4® T4 Series Touchscreens | Datasheet, CONTROL4, *accessible as a pdf at* https://www.control4.com/docs/product/t4-series-touchscreen/data-sheet/english/latest (last accessed Nov. 15, 2022).

33. The Defendants' remotes, such as the Control4 Neeo Remote shown below,"[c]ontrol[] audio and video equipment, along with lights, music, temperature, shades, and more," via a Wi-Fi connection to a wireless network.

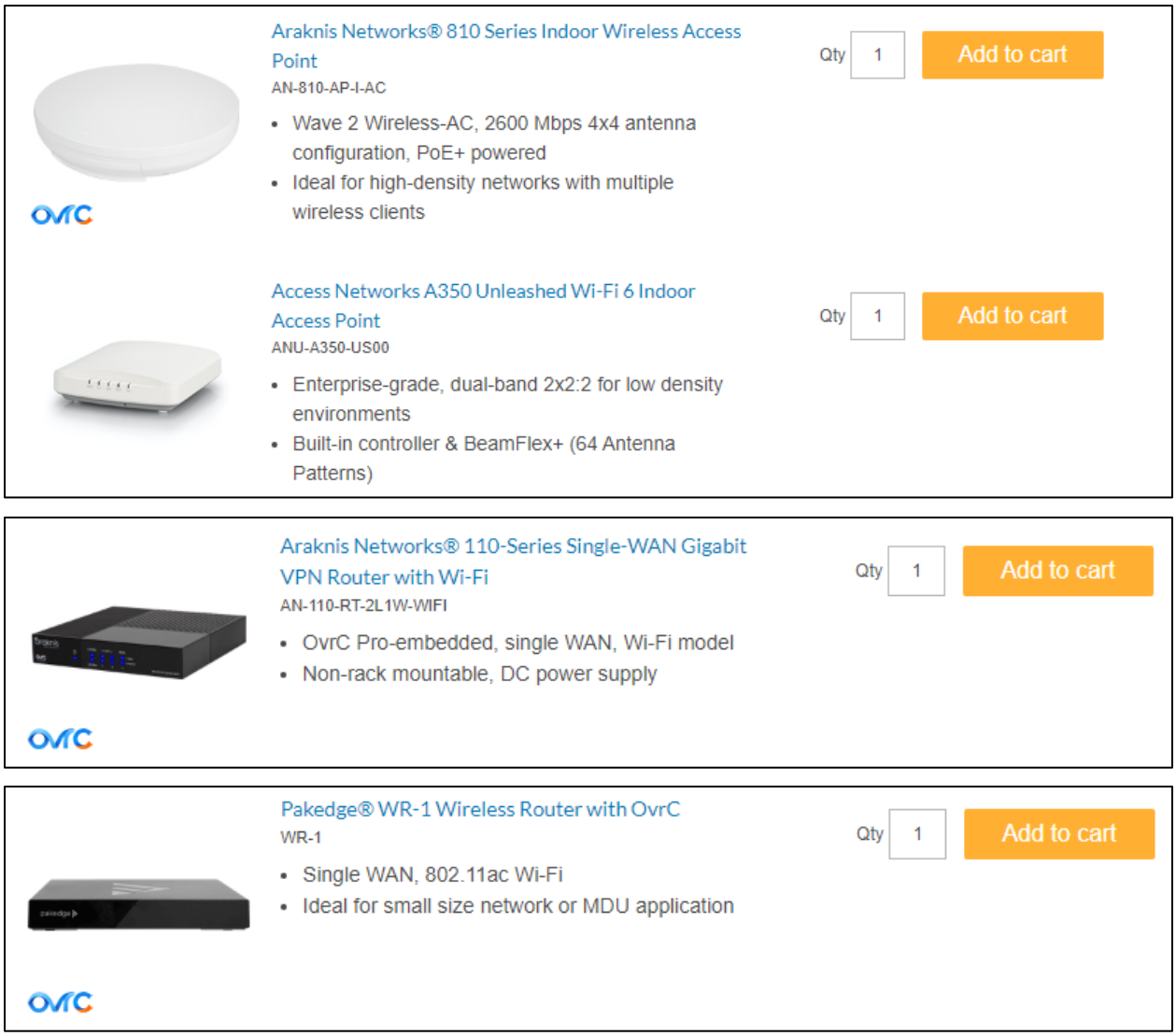
Ports and interfaces	• WiFi (802.11b/g/n) • Accelerometer • Charging connector (gold plated)

Neeo Remote for Control4| Datasheet, CONTROL4, *accessible as a pdf at* https://www.control4.com/docs/product/neeo-remote/data-sheet/english/latest (last accessed Nov. 15, 2022).

34. The Asserted Patents cover Defendants' "Networking Access Points" which are at least sold under the pakedge® brand. As shown below, these access points are touted by Defendants as "provid[ing] reliable, worry-free networking for today's connected home," via their connection to a wireless Wi-Fi network. *Worry-Free Wireless, Designed for AV*, PAKEDGE, https://pakedge.com/products/wireless/ (last visited Nov. 15, 2022).

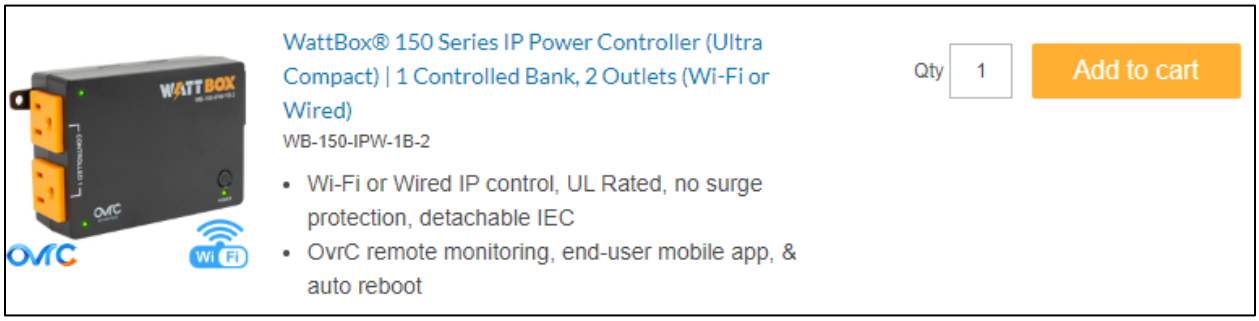
Id.

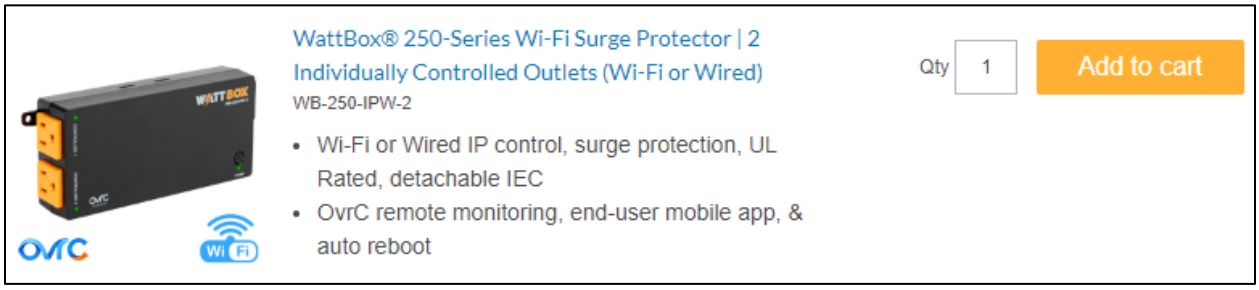
35. As shown below, Defendants also provide Araknis-branded access points and routers which are configured to connect to a wireless Wi-Fi network. *Access Points*, SNAP ONE, https://www.snapav.com/shop/en/snapav/search/access-points (last visited Nov. 18, 2022); *Routers*, SNAP ONE, https://www.snapav.com/shop/en/snapav/search/routers (last visited Nov. 16, 2022).



Id.

36. The Asserted Patents cover Defendants' "power controllers" and "surge protectors" which include WattBox® branded devices that have "wireless capability [that] can power and control everything from digital signage or a smart TV to video conferencing equipment or an entire A/V rack." *IP Power*, SNAP ONE, https://www.snapav.com/shop/en/snapav/search/ip-power (last visited Nov. 16, 2022). For example, the WattBox® 150 Series and WattBox® 350 Series provide Wi-Fi control and is supported by Snap One's OvrC "remote monitoring, end-user mobile app.





Id.

37. The Accused Products utilize intrusion detection methods for a local or metropolitan area network to infringe at least the ’678,’572, and ’126 patents. For example, the IEEE 802.11 authentication methods utilized by the Accused Products include a TKIP-based method, as explained below, that uses a “MIC” to defend against active attacks to provide a secure wireless network.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

8.3.2.3 TKIP MIC

Flaws in the IEEE 802.11 WEP design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer as described in 8.6.1 and 8.6.2.

Annex H contains an implementation of the TKIP MIC. It also provides test vectors for the MIC.

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates. Active attacks enabled by the original WEP design include the following:

— Bit-flipping attacks
— Data (payload) truncation, concatenation, and splicing
— Fragmentation attacks
— Iterative guessing attacks against the key
— Redirection by modifying the MPDU DA or RA field
— Impersonation attacks by modifying the MPDU SA or TA field

The MIC makes it more difficult for any of these attacks to succeed.

All of these attacks remain at the MPDU level with the TKIP MIC. The MIC, however, applies to the MSDU, so it blocks successful MPDU-level attacks. TKIP applies the MIC to the MSDU at the transmitter and verifies it at the MSDU level at the receiver. If a MIC check fails at the MSDU level, the implementation shall discard the MSDU and invoke countermeasures (see 8.3.2.4).

Page 217, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

38. Stations (STAs) in an IEEE 802.11 network of the Accused Products associate with each other using a robust security network association (RSNA). As described below, RSNA supports intrusion detection by employing authentication mechanisms and data frame protection mechanisms (such as, temporal key integrity protocol – TKIP and CCMP) between the STAs. Data is exchanged between the STAs in the form of MPDUs (medium access control (MAC) protocol data units). The MAC frame (MPDU) comprises a MSDU (information frame) in the frame body,

and four addresses that identify, among others, source MAC address (SA) and destination MAC address (DA) for the MSDU.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

5.1.1.4 Interaction with other IEEE 802® layers

IEEE Std 802.11 is required to appear to higher layers [logical link control (LLC)] as a wired IEEE 802 LAN. This requires that the IEEE 802.11 network handle STA mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE Std 802.11 to incorporate functionality that is untraditional for MAC sublayers.

In a robust security network association (RSNA), IEEE Std 802.11 provides functions to protect data frames, IEEE Std 802.1X-2004 provides authentication and a Controlled Port, and IEEE Std 802.11 and IEEE Std 802.1X-2004 collaborate to provide key management. All STAs in an RSNA have a corresponding IEEE 802.1X entity that handles these services. This standard defines how an RSNA utilizes IEEE Std 802.1X-2004 to access these services.

3.126 robust security network (RSN): A security network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN information element (IE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).

3.127 robust security network association (RSNA): The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake. Note that the existence of an RSNA by a pair of devices does not of itself provide robust security. Robust security is provided when all devices in the network use RSNAs.

5.2.3.2 RSNA

An RSNA defines a number of security features in addition to wired equivalent privacy (WEP) and IEEE 802.11 authentication. These features include the following:

- Enhanced authentication mechanisms for STAs
- Key management algorithms
- Cryptographic key establishment
- An enhanced data cryptographic encapsulation mechanism, called Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP), and, optionally, Temporal Key Integrity Protocol (TKIP).

Page 72, 61, 75 https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

39. In the TKIP method of the Accused Products, an MSDU transmitter STA calculates cryptographic message integrity code (MIC) using the MAC addresses (SA & DA) corresponding to the MSDU. As described below, the transmission is monitored if the MIC (which is obtained using the MAC addresses) is verified/authenticated at the receiver. MSDUs with invalid MICs are discarded and countermeasures are invoked.

8.3 RSNA data confidentiality protocols

8.3.1 Overview

This standard defines two RSNA data confidentiality and integrity protocols: TKIP and CCMP. Implementation of CCMP shall be mandatory in all IEEE 802.11 devices claiming RSNA compliance. Implementation of TKIP is optional for an RSNA. A design aim for TKIP was that the algorithm should be implementable within the capabilities of most devices supporting only WEP, so that many such devices would be field-upgradeable by the supplier to support TKIP.

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1 TKIP overview

The TKIP is a cipher suite enhancing the WEP protocol on pre-RSNA hardware. TKIP modifies WEP as follows:

a) A transmitter calculates a keyed cryptographic message integrity code (MIC) over the MSDU SA and DA, the MSDU priority (see 8.3.2.3), and the MSDU plaintext data. TKIP appends the computed MIC to the MSDU data prior to fragmentation into MPDUs. The receiver verifies the MIC after decryption, ICV checking, and defragmentation of the MPDUs into an MSDU and discards any received MSDUs with invalid MICs. TKIP's MIC provides a defense against forgery attacks.

b) Because of the design constraints of the TKIP MIC, it is still possible for an adversary to compromise message integrity; therefore, TKIP also implements countermeasures. The countermeasures bound the probability of a successful forgery and the amount of information an attacker can learn about a key.

Page 213, 214 https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

40. The TKIP MIC implementation of the Accused Products prevents intrusion attacks, such as, message redirection by modifying destination/receiver MAC address (DA or RA) and impersonation by modifying the source/transmitter MAC address (SA or TA). As described below, the transmission is monitored if the MIC (which is obtained using the MAC addresses) is

verified/authenticated at the receiver. MSDU with an invalid MIC will indicate a modified MAC address (SA or DA), thereby resulting in discarding the MSDU and invoking the countermeasures.

8.3.2.3 TKIP MIC

Flaws in the IEEE 802.11 WEP design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer as described in 8.6.1 and 8.6.2.

Annex H contains an implementation of the TKIP MIC. It also provides test vectors for the MIC.

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates. Active attacks enabled by the original WEP design include the following:

- Bit-flipping attacks
- Data (payload) truncation, concatenation, and splicing
- Fragmentation attacks
- Iterative guessing attacks against the key
- Redirection by modifying the MPDU DA or RA field
- Impersonation attacks by modifying the MPDU SA or TA field

The MIC makes it more difficult for any of these attacks to succeed.

All of these attacks remain at the MPDU level with the TKIP MIC. The MIC, however, applies to the MSDU, so it blocks successful MPDU-level attacks. TKIP applies the MIC to the MSDU at the transmitter and verifies it at the MSDU level at the receiver. If a MIC check fails at the MSDU level, the implementation shall discard the MSDU and invoke countermeasures (see 8.3.2.4).

Page 217, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

41. Upon detecting a first MIC failure, as described below, a countermeasure timer is initiated, and a failure event (alert) is reported to the AP by sending a Michael MIC Failure Report frame. Upon detecting a second consecutive MIC failure within 60 seconds, i.e., detecting a number of failed attempts, the participating STAs are deauthenticated, wherein deauthentication involves

sending a notification (i.e., generating an alert) to deauthenticate due to an intrusion (2 consecutive MIC failures has occurred).

8.3.2.4 TKIP countermeasures procedures

The TKIP MIC trades off security in favor of implementability on pre-RSNA devices. Michael provides only weak protection against active attacks. A failure of the MIC in a received MSDU indicates a probable active attack. A successful attack against the MIC would mean an attacker could inject forged data frames and perform further effective attacks against the encryption key itself. If TKIP implementation detects a probable active attack, TKIP shall take countermeasures as specified in this subclause. These countermeasures accomplish the following goals:

— MIC failure events *should* be logged as a security-relevant matter. A MIC failure is an almost certain indication of an active attack and warrants a follow-up by the system administrator.

— The rate of MIC failures *must* be kept below two per minute. This implies that STAs and APs detecting two MIC failure events within 60 s must disable all receptions using TKIP for a period of 60 s. The slowdown makes it difficult for an attacker to make a large number of forgery attempts in a short time.

A single counter or timer shall be used to log MIC failure events. These failure events are defined as follows:

— For an Authenticator:
  — Detection of a MIC failure on a received unicast frame.
  — Receipt of Michael MIC Failure Report frame.
— For a Supplicant:
  — Detection of a MIC failure on a received unicast or broadcast/multicast frame.
  — Attempt to transmit a Michael MIC Failure Report frame.

The number of MIC failures is accrued independent of the particular key context. Any single MIC failure, whether detected by the Supplicant or the Authenticator and whether resulting from a group MIC key failure or a pairwise MIC key failure, shall be treated as cause for a MIC failure event.

The Supplicant uses a single Michael MIC Failure Report frame to report a MIC failure event to the Authenticator. A Michael MIC Failure Report is an EAPOL-Key frame with the following Key Information

The first MIC failure shall be logged, and a timer initiated to enable enforcement of the countermeasures. If the MIC failure event is detected by the Supplicant, it shall also report the event to the AP by sending a Michael MIC Failure Report frame.

If a subsequent MIC failure occurs within 60 s of the most recent previous failure, then a STA whose IEEE 802.1X entity has acted as a Supplicant shall deauthenticate (as defined in 11.3.1.3) itself or deauthenticate all the STAs with a security association if its IEEE 802.1X entity acted as an Authenticator. For an IBSS STA, both Supplicant and Authenticator actions shall be taken. Furthermore, the device shall not receive or transmit any TKIP-encrypted data frames, and shall not receive or transmit any unencrypted data frames other than IEEE 802.1X messages, to or from any peer for a period of at least 60 s after it detects the second failure. If the device is an AP, it shall disallow new associations using TKIP during this 60 s period; at the

Page 219, 220, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

42. The Asserted Patents cover Snap One's Accused Products that are Wi-Fi compliant devices and support WPA, WPA2 and WPA3 security mechanisms, as described below and in the

following paragraphs. The WPA mechanism is based on Temporal Key Integrity Protocol (TKIP), while the WPA2 and WPA3 are based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).

43. Defendants configure their infringing Accused Products to not only connect to Wi-Fi compliant networks, but also to utilize authentication techniques such as WPA (TKIP) and WPA2 (CCMP) for secure connections to those wireless networks. As shown below, Snap One's Conrol4 EA-5 is configured to connect to wireless networks via Wi-Fi and utilized Wi-Fi Security measures shown as WPA and WPA2.

Network	
Ethernet	10/100/1000BaseT compatible (required for controller setup)
Built-in Ethernet switch	1 Ethernet in + 4 gigabit Ethernet switch ports
WiFi	Internal Dual-Band Wireless-N (EA-5 V1) (2.4 GHz, 5 GHz, 802.11n/g/b) Optional Dual-Band WiFi USB Adapter (EA-5 V2) (2.4 GHz, 5 Ghz, 802.11ac/b/g/n/a)
WiFi security	WPA/WPA2
WiFi antenna	External reverse SMA connector (EA-5 V1 only); optional WiFi adapter on the EA-5 V2

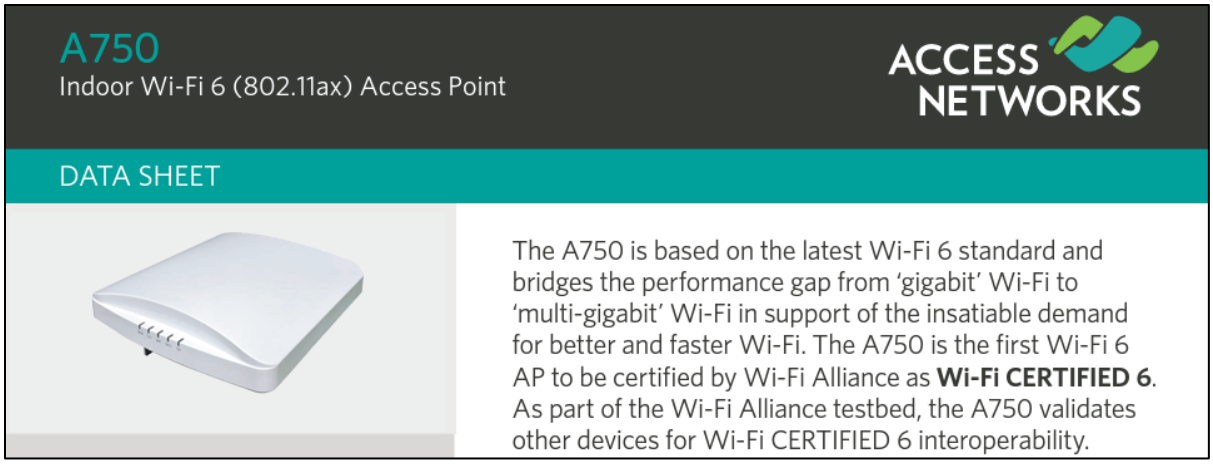
Control4® EA-5 Controller, | *Datasheet*, SNAP ONE, *available as a pdf file at* https://www.control4.com/solutions/products/controllers (last visited Nov. 16, 2022).

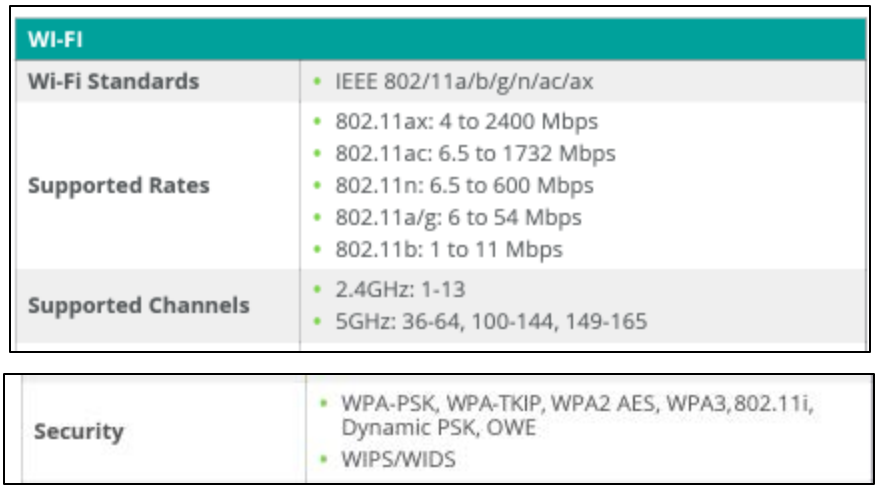
44. Also, Snap One's touchscreens, such as the Control4 T4 Series Touchscreens also utilize authentication techniques such as WPA (TKIP) and WPA2 (CCMP) for secure connections to those wireless networks, as shown below.

Features	
Screen	Resolution: 1920 1200 Capacitive touch Camera: 720p
Wireless network	802.11b/g/n 2.4 GHz 802.11a/n/ac 5 GHz Security: WEP, WPA/WPA2 PSK, 802.1x EAP, PEAP

Touchscreens, CONTROL4, https://www.control4.com/solutions/products/touchscreens/ (datasheet for the Control T4 Series Touchscreen available via the "Spec Sheet" button).

45. Snap One's networking products, such as the Access Networks branded A750 Access Point shown below, also not only connect devices over a wireless Wi-Fi network, but also provide network security features, including WPA-TKIP, WPA2 AES, and WPA3.





See A750 Indoor Wi-Fi 6 (802.11ax) Access Point | Data Sheet, ACCESS NETWORKS, *available for download at* https://www.accessnetworks.com/wp-content/uploads/2022/06/AN_A750-Data-Sheet.pdf (last access on Nov. 18, 2022).

46. As shown above, the Accused Products provide wireless connectivity utilizing the 802.11 protocols at one or both of 2.4 GHz and/or 5 GHz Wi-Fi speeds. This capability ascertains the presence of a MAC controller, a Wi-Fi antenna, and a transceiver in the device and provides a secure wireless LAN.

47. The Accused Products further utilize a cryptography circuit that implements the 802.11 protocols authentication techniques, including TKIP and CCMP. Shown below is a block diagram from the 802.11 protocol documentation showing the TKIP-based cryptography circuit (such as used with WPA) that is utilized in the Accused Products. The circuit shown encrypts both address (destination address (DA), source address (SA)) and data information (plaintext MSDU)

by adding encryptions bits (MIC key) to both the address and data. The cryptography circuit of the Accused Products is also configured to decrypt the encrypted address and data information.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1.1 TKIP cryptographic encapsulation

TKIP enhances the WEP cryptographic encapsulation with several additional functions, as depicted in Figure 8-4.

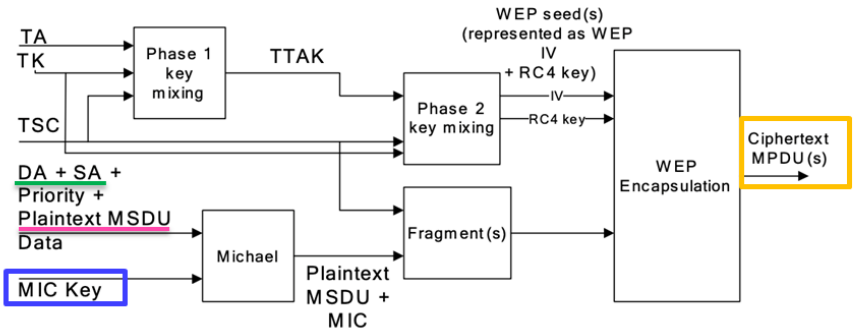


Figure 8-4—TKIP encapsulation block diagram

a) TKIP MIC computation protects the MSDU Data field and corresponding SA, DA, and Priority fields. The computation of the MIC is performed on the ordered concatenation of the SA, DA, Priority, and MSDU Data fields. The MIC is appended to the MSDU Data field. TKIP discards any MIC padding prior to appending the MIC.

b) If needed, IEEE Std 802.11 fragments the MSDU with MIC into one or more MPDUs. TKIP assigns a monotonically increasing TSC value to each MPDU, taking care that all the MPDUs generated from the same MSDU have the same value of extended IV (see 8.3.2.2).

c) For each MPDU, TKIP uses the key mixing function to compute the WEP seed.

d) TKIP represents the WEP seed as a WEP IV and ARC4 key and passes these with each MPDU to WEP for generation of the ICV (see 7.1.3.6), and for encryption of the plaintext MPDU, including all or part of the MIC, if present. WEP uses the WEP seed as a WEP default key, identified by a key identifier associated with the temporal key.

Page 213, 214, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

48. Shown below is a block diagram from the 802.11 protocol documentation showing the CCMP-based cryptography circuit (such as used with WPA2) that is utilized in the Accused Products. The circuit shown encrypts both address (A2 – MPDU address 2) and data information (plaintext MPDU) by adding encryptions bits (temporal key (TK)) to both the address and data. The

cryptography circuit of the Accused Products is also configured to decrypt the encrypted address and data information.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

8.3.3.3 CCMP cryptographic encapsulation

The CCMP cryptographic encapsulation process is depicted in Figure 8-16.

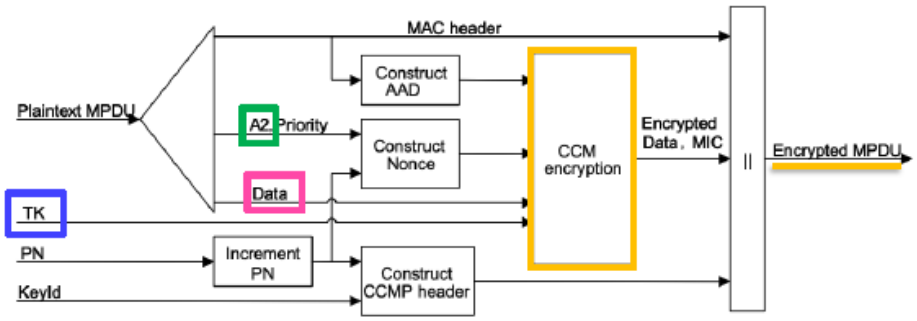


Figure 8-16—CCMP encapsulation block diagram

CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting cipher text using the following steps:

a) Increment the PN, to obtain a fresh PN for each MPDU, so that the PN never repeats for the same temporal key. Note that retransmitted MPDUs are not modified on retransmission.

b) Use the fields in the MPDU header to construct the additional authentication data (AAD) for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD. MPDU header fields that may change when retransmitted are muted by being masked to 0 when calculating the AAD.

c) Construct the CCM Nonce block from the PN, A2, and the Priority field of the MPDU where A2 is MPDU Address 2.

d) Place the new PN and the key identifier into the 8-octet CCMP header.

e) Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and MIC. This step is known as CCM originator processing.

f) Form the encrypted MPDU by combining the original MPDU header, the CCMP header, the encrypted data and MIC, as described in 8.3.3.2.

Page 229, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

49. Defendants also infringe the ’126 patent by providing products that utilize a volatile memory for storing cryptography information utilized in the cryptography circuit and a battery for maintaining the cryptography in the volatile memory, including via at least security control panels and keypads (e.g., the ClareOne Wireless Security and Smart Home Panel, model no. CLR-C1-PNL1), Tabletop Touch Screens (e.g., the Control 4 T3-7), and the Neeo Remote for Control4.

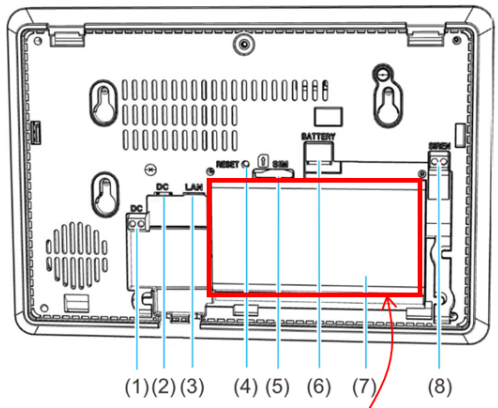
50. On information and belief, the entity "Clare Controls" sells security and smart home products under the ClareOne trademark in the U.S. Moreover, Clare Controls is a business segment of Defendant Snap One, LLC, which does business under the name "Clare Controls." *See Clare*, CLARE CONTROLS, htttp://www.clarecontrols.com (stating "Snap One, LLC dba Clare Controls" holds the copyright for the website) (last visited Dec. 15, 2022).

51. As shown in the User Manual for Snap One's ClareOne-branded Wireless Security and Smart Home Panel, the panel utilizes a battery that provides power to maintain data for "24 hours." On information and belief, the battery maintains cryptographic information in the product's internal (volatile) memory. Such cryptographic information allows data encryption to be carried out over a secure wireless 802.11 network.

ClareOne Wireless Security and Smart Home Panel User Manual

Model CLR-C1-PNL1

Figure 3: ClareOne Panel - interior rear



(1) DC wiring terminal
(2) DC micro USB port
(3) LAN port (USB-C)
(4) Panel reset hole
(5) SIM card slot
(6) Battery connection
(7) Battery
(8) Siren wiring terminal

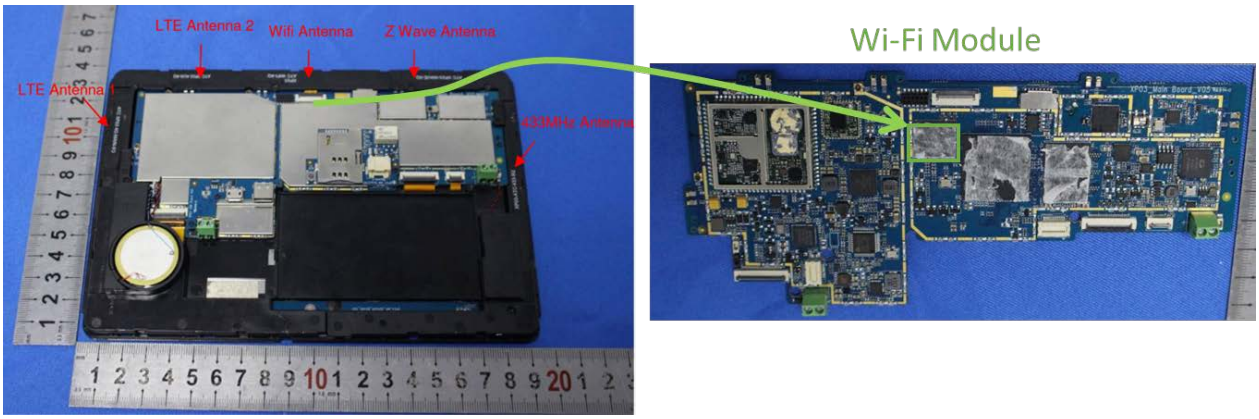
Power options

The panel can be powered by the provided power supply with a micro USB cable, using the provided power supply with Cat5/6 cable, or using the provided power supply with 22AWG or thicker shielded security wiring. For details on the ClareOne panel power options, see Power supply options on page 9.

Note: In the case of a power outage, the battery in the panel lasts 24 hours plus an additional 4 minutes of alarm signaling.

See ClareOne Wireless Security and Smart Home Panel User Manual, Clare Controls, LLC | Model CLR-C1-PNL1.

52. Furthermore, as shown below in pictures of a teardown of Snap One's ClareOne-branded Wireless Security and Smart Home Panel submitted to the FCC, the controller for the product includes a Wi-Fi module that has an internal volatile memory for storing data, including cryptographic information.

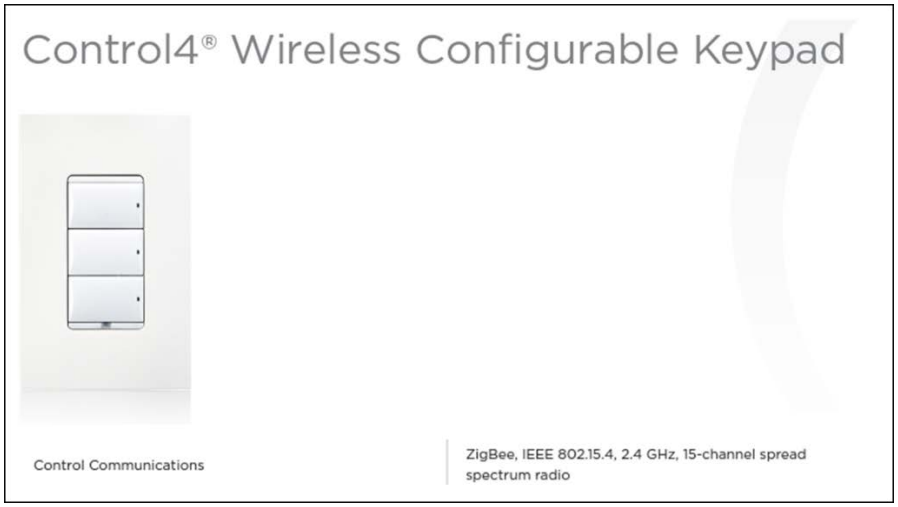


See Clare Controls Wireless Security and Smart Home Panel C1-PNL1 | FCC ID 2AC9I-C1-PNL1, FCC.ID, *internal photos accessible as a pdf file at* https://fccid.io/2AC9I-C1-PNL1 (last visited Dec. 21, 2022)

53. Defendants also infringe the '961 patent via Snap One products that use the ZigBee protocol to communicate with other devices on the network, including those devices of third-party manufacturers. ZigBee protocol is based on the IEEE 802.15.4 standard. *See Control4 EA5 Controller | Datasheet, Control4, available as a pdf file at* https://www.control4.com/solutions/products/controllers ("Secure, wireless Zigbee communication; plentiful I/O including IR, serial, contacts and relays; and IP control enable connections to smart home devices such as thermostats, door locks, doorbells, cameras, security panels, sensors, lighting, shades, garage door controllers, irrigation systems, and much more." (last visited Nov. 16, 2022). An example of Snap One's Control4 EA-5 Controller is shown below:

Zigbee Pro	802.15.4
ZigBee antenna	External reverse SMA connector

54. Snap One's ZigBee-enabled controllers provide a platform to utilize other Snap One products that communicate over a ZigBee wireless network, including the Control4® Wireless Configurable Keypad, Wireless Keypad Dimmer, Wireless Thermostat, Fan Speed Controller, and Sensors, as shown below.



Control4® Wireless Keypad Dimmer

Control communications	ZigBee, IEEE 802.15.4, 2.4 GHz, 15-channel, spread-spectrum radio

Control4® Wireless Thermostat by Aprilaire®

Control communications	ZigBee (IEEE 802.15.4), 2.4 GHz mesh networking

Control4® Wireless Fan Speed Controller

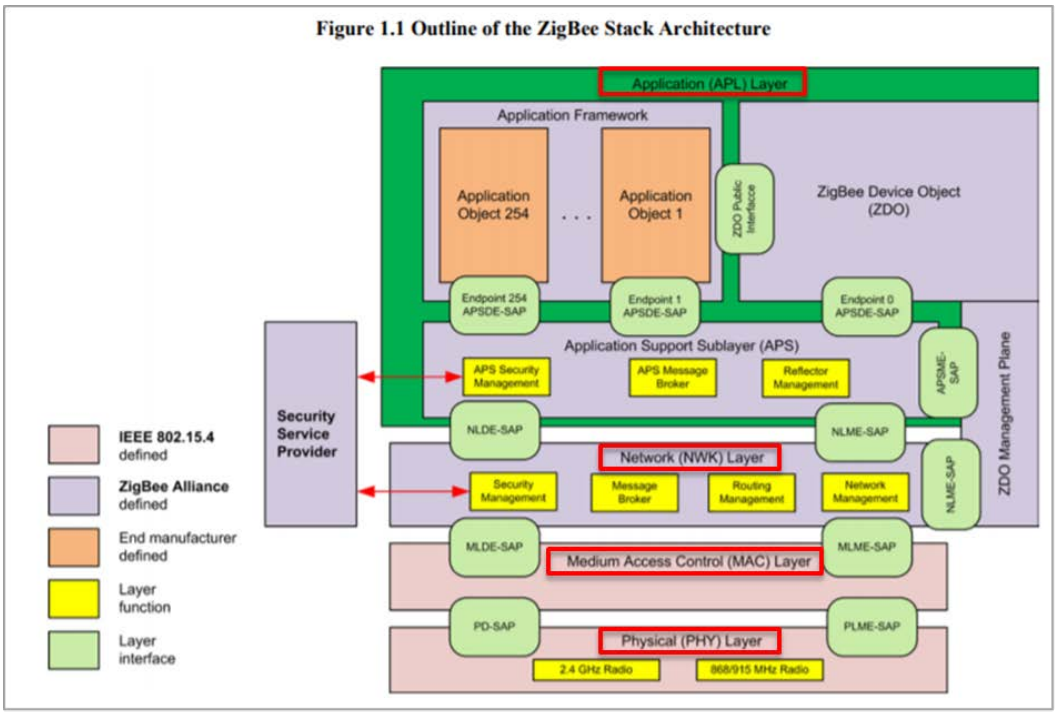
Control Communications	ZigBee, IEEE 802.15.4, 2.4 GHz, 15-channel spread spectrum radio

MOTION SENSOR

The Wireless Motion Sensors communicate motion and ambient light events to the Control4 system using ZigBee®. Based on room occupancy you can trigger and control events throughout the Control4 system. Sensing motion and light inside and outside the home gives you automation control that responds to movement or changes in ambient light levels.

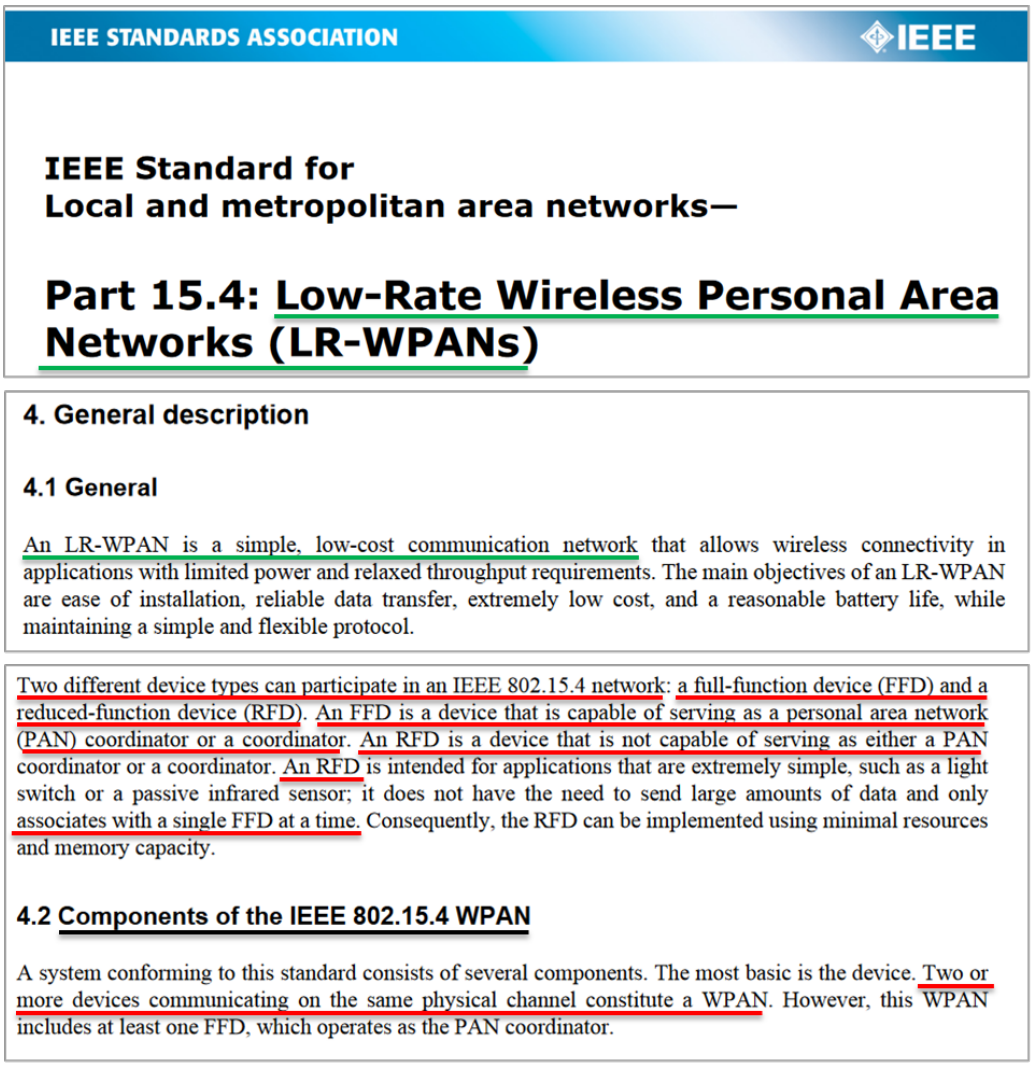
See, e.g., *Product Catalog*, CONTROL4, https://www.control4.com/solutions/catalog (providing links for each type of product listed above).

55. Zigbee is a low-power, two-way, wireless communication standard that is used to implement a mobile ad hoc network. Zigbee network stack consists of Application Layer, Network Layer, MAC Layer, and Physical (PHY) Layer.



Page 24, 25, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

56. The IEEE 802.15.4 standard based mobile ad-hoc network, i.e., ZigBee, utilized by the Accused Products, is a type of Low-Rate Wireless Personal Area Network (LR-WPAN) that allows transmission of data between plurality of network nodes.



IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for
Local and metropolitan area networks—

Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)

4. General description

4.1 General

An LR-WPAN is a simple, low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. The main objectives of an LR-WPAN are ease of installation, reliable data transfer, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol.

Two different device types can participate in an IEEE 802.15.4 network: a full-function device (FFD) and a reduced-function device (RFD). An FFD is a device that is capable of serving as a personal area network (PAN) coordinator or a coordinator. An RFD is a device that is not capable of serving as either a PAN coordinator or a coordinator. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor; it does not have the need to send large amounts of data and only associates with a single FFD at a time. Consequently, the RFD can be implemented using minimal resources and memory capacity.

4.2 Components of the IEEE 802.15.4 WPAN

A system conforming to this standard consists of several components. The most basic is the device. Two or more devices communicating on the same physical channel constitute a WPAN. However, this WPAN includes at least one FFD, which operates as the PAN coordinator.

Page 8, http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf

57. The Accused Products, including the Snap One products utilizing the ZigBee protocol identified above, practice a method for dynamic channel allocation in a mobile ad hoc network. As indicated below, "[a] single device can become the Network Channel Manager."

ANNEX E

OPERATING NETWORK MANAGER AS NETWORK CHANNEL MANAGER FOR INTERFERENCE REPORTING AND RESOLUTION

ZigBee Control your world

A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated by sending a Mgmt_NWK_Update_req command with a different short address for the network channel manager. The device that is the Network Channel Manager shall set the network manager bit in the server mask in the node descriptor and shall respond to System_Server_Discovery_req commands.

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause. The following steps are an example of that procedure[1]:

1. Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.
2. If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent as an APS Unicast with acknowledgement and once the acknowledgment is received the total transmit and transmit failure counters are reset to zero.

Page 516, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

58. As shown below, in different ZigBee Network topologies of the Accused Products, a plurality of network nodes is connected together via a respective plurality communication links.

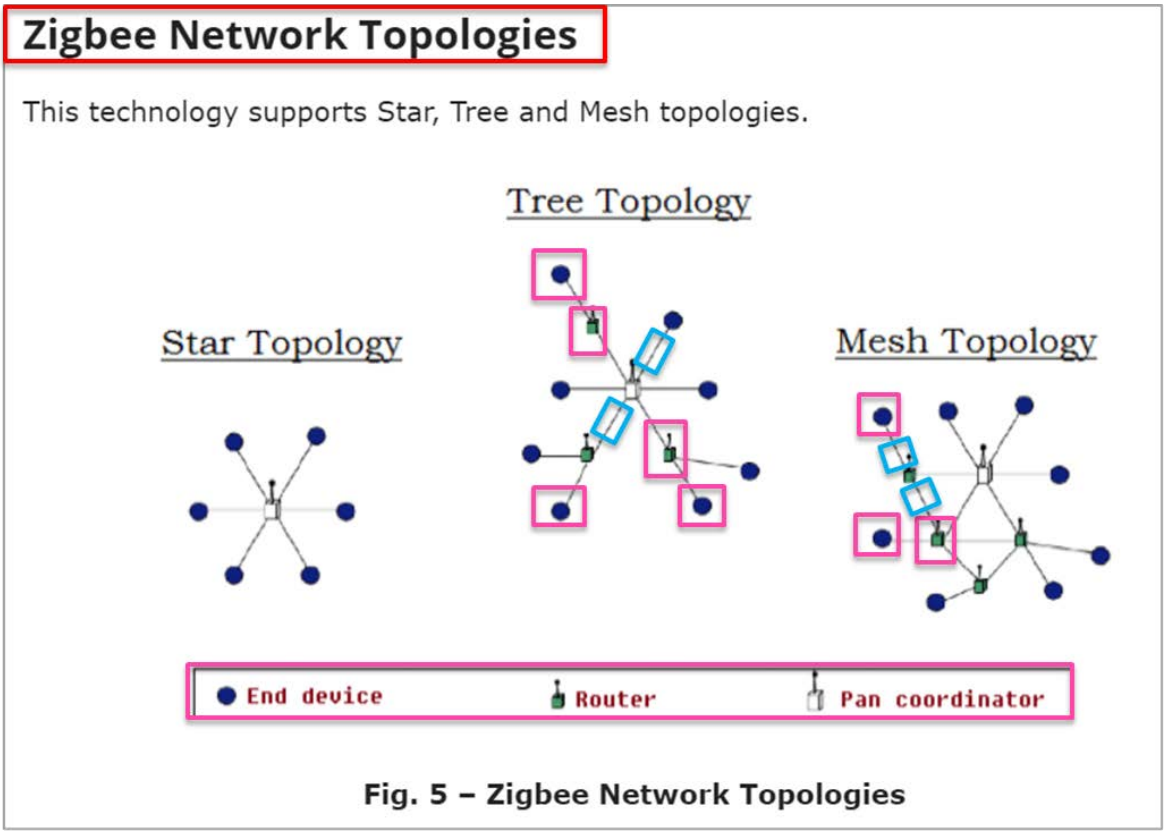


Fig. 5 – Zigbee Network Topologies

https://electricalfundablog.com/zigbee-technology-architecture/

59. In the ZigBee network of the Accused Products, a network device/node is configured to monitor the performance of a channel-in-use based on its energy measurement. As described below, if the measurement value is higher than the value on other channels (threshold), it indicates interference is present on the channel, consequently resulting in transmission failures.

ZigBee Control your world

ANNEX E OPERATING NETWORK MANAGER AS NETWORK CHANNEL MANAGER FOR INTERFERENCE REPORTING AND RESOLUTION

A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated by sending a Mgmt_NWK_Update_req command with a different short address for the network channel manager. The device that is the Network Channel Manager shall set the network manager bit in the server mask in the node descriptor and shall respond to System_Server_Discovery_req commands.

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause. The following steps are an example of that procedure[1]:

1. Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.
2. If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent as an APS Unicast with acknowledgement and once the acknowledgment is received the total transmit and transmit failure counters are reset to zero.

Page 516, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

60. As described below, the network manager node facilitates switching to a different channel, i.e., scouting available separate channels, if the performance on the channel-in-use falls below a threshold (i.e., when the current channel's energy is higher than channels, indicating increased interference, and thereby resulting in multiple transmission failures). The network nodes switch to a new (second) channel whose energy level is lowest or below an acceptable threshold.

ZigBee Control your world

A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated by sending a Mgmt_NWK_Update_req command with a different short address for the network channel manager. The device that is the Network Channel Manager shall set the network_manager_bit in the server mask in the node descriptor and shall respond to System_Server_Discovery_req commands.

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause. The following steps are an example of that procedure[1]:

1. Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.
2. If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent as an APS Unicast with acknowledgement and once the acknowledgment is received the total transmit and transmit failure counters are reset to zero.
3. To avoid a device with communication problems from constantly sending reports to the network manager, the device should not send a Mgmt_NWK_Update_notify more than 4 times per hour.

Upon receipt of an unsolicited Mgmt_NWK_Update_notify, the network manager must evaluate if a channel change is required in the network. The specific mechanisms the network manager uses to decide upon a channel change are left to the implementers. It is expected that implementers will apply different methods to best determine when a channel change is required and how to select the most appropriate channel. The following is offered as guidance for implementation.

Comment: *Zigbee network further allows network devices/nodes to function as Network Channel Manager. The network manager node facilitates switching to a different channel if the performance on the channel-in-use falls below a threshold (i.e., when the current channel's energy is higher than channels, indicating increased interference, and thereby resulting in multiple transmission failures).*

Page 516, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

61. With reference to the above graphic and as further described below, the ZigBee network of the Accused Products further allows using the command to request interference reports, i.e., broadcasts a channel activity query, from the network nodes, which involves scanning the energy level on all the channels including the newly switched (second) channel. The interference report will represent determining the performance for the second channel. In addition, the most

recent energy level value and failure rate (indicative of the channel performance/activity) corresponding to the channels is stored, i.e., the channel activity is updated.

The network manager may do the following:

1. Wait and evaluate if other reports from other devices are received. This may be appropriate if there are no other failures reported. In this case the network manager should add the reporting device to a list of devices that have reported interference. The number of devices on such a list would depend on the size of the network. The network manager can age devices out of this list.
2. Request other interference reports using the Mgmt_NWK_Update_req command. This may be done if other failures have been reported or the network manager device itself has failures and a channel change may be desired. The network manager may request data from the list of devices that have reported interference plus other randomly selected routers in the network. The network manager should not request an update from the device that has just reported interference since this data is fresh already.
3. Upon receipt of the Mgmt_NWK_Update_notify, the network manager shall determine if a channel change is required using whatever implementation specific mechanisms are considered appropriate. The network manager device with just one channel allowed in the *apsChannelMask* parameter must not issue the Mgmt_Nwk_Update_Req command to request other devices to change the current channel. However, the network manager may report channel quality issues to the application.
4. If the above data indicate a channel change should be considered, the network manager completed the following:
   a. Select a single channel based on the Mgmt_NWK_Update_notify based on the lowest energy. This is the proposed new channel. If this new channel does not have an energy level below an acceptable threshold, a channel change should not be done. Additionally, a new channel shall not belong to a PHY different from the one on which a network manager is operating now.
5. Prior to changing channels, the network manager should store the energy scan value as the last energy scan value and the failure rate from the existing channel as the last failure rate. These values are useful to allow comparison of the failure rate and energy level on the previous channel to evaluate if the network is causing its own interference.
6. The network manager should broadcast a Mgmt_NWK_Update_req notifying devices of the new channel. The broadcast shall be to all devices with RxOnWhenIdle equal to TRUE. The network manager is responsible for incrementing the *nwkUpdateId* parameter from the NIB and including it in the Mgmt_NWK_Update_req. The network manager shall set a timer based on the value of *apsChannelTimer* upon issue of a Mgmt_NWK_Update_req that changes channels and shall not issue another such command until this timer expires. However, during this period, the network manager can complete the above analysis. However, instead of changing channels, the network manager would report to the local application using Mgmt_NWK_Update_notify and the application can force a channel change using the Mgmt_NWK_Update_req.

Upon receipt of a Mgmt_NWK_Update_req with a change of channels, the local network manager shall set a timer equal to the *nwkNetworkBroadcastDeliveryTime* and shall switch channels upon expiration of this timer. Each node shall also increment the *nwkUpdateId* parameter and also reset the total transmit count and the transmit failure counters.

Page 517, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

COUNT I

(INFRINGEMENT OF U.S. PATENT NO. 7,224,678)

62. Plaintiff incorporates paragraphs 1 through 61 herein by reference.

63. Plaintiff is the assignee of the ’678 patent, entitled “Wireless local or metropolitan area network with intrusion detection features and related methods,” with ownership of all substantial rights in the ’678 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

64. The ’678 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The ’678 patent issued from U.S. Patent Application No. 10/217,042.

65. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the ’678 patent in this District and elsewhere in Texas and the United States.

66. On information and belief, the Snap One Defendants design, develop, manufacture, import, distribute, offer to sell, sell, and use the Accused Products, including via the activities of Snap Holdings and its subsidiaries, members, segments, companies, brands and/or related entities, such as Defendant Snap LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One.

67. Defendants each directly infringe the ’678 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the ’678 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or

consumers. Furthermore, on information and belief, Defendants design the Accused Products for U.S. consumers, make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, installers, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '678 patent. *See, e.g.*, *Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

68. Furthermore, Defendant Snap Holdings directly infringes the '678 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant Snap LLC, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One, including by designing the Accused Products for U.S. consumers and selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, Snap One's U.S.-based subsidiaries, including at least Snap LLC, conduct activities that constitute direct infringement of the '678 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants, including parent company Snap Holdings. Defendant Snap Holdings is vicariously liable for the infringing conduct of Defendant Snap LLC and other U.S.-based subsidiaries, members, business segments, companies and/or brands of Snap One (under both the alter ego and agency theories). On information and belief,

Defendants Snap Holdings, Snap LLC, and other U.S. based subsidiaries members, segments, companies and/or brands of Snap One are essentially the same company (i.e., "Snap One"), operating in the U.S. via at least the Control4™, araknis™, Access Networks®, pakedge®, Clare™, WattBox®, SunbriteTV™, and Allnet™ brands, segments, mergers, or acquisitions of Snap One. Moreover, Snap Holdings, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendants each receive a direct financial benefit from that infringement.

69. Defendants infringe claim 51 of the '678 patent via the Accused Products that utilize or are enabled with or compliant with 802.11 (Wi-Fi) protocols, including, but not limited to Defendants' security, smart home, networking, and automation products, such as smart home systems, controllers, touchscreens, wireless keypads, dimmers, remotes, access points, routers, security cameras, power controllers, surge protectors, components, software/firmware, services, processes, related accessories, and mobile applications.

70. Those Accused Products include "[a]n intrusion detection method for a wireless local or metropolitan area network comprising a plurality of stations" comprising the limitations of claim 51. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include the steps of transmitting data between the plurality of stations using a media access layer (MAC), each of the stations having a respective MAC address associated therewith; monitoring transmissions among the plurality of stations to detect failed attempts to authenticate MAC addresses; and generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address.

71. At a minimum, Defendants have known of the ’678 patent at least as early as the filing date of this complaint. In addition, Defendants have known about their infringement of L3Harris Corporation’s patent portfolio which Stingray now owns and includes the ’678 patent, since at least its receipt of a letter from Acacia Research Group on behalf of Stingray to Snap One’s predecessor Control4 Corporation, dated July 29, 2020. Stingray also contacted Snap One on April 28, 2021 alleging infringement of patents in the Stingray portfolio. These letters notify Defendants that their products practice at least ZigBee and Wi-Fi wireless network technologies covered by the Stingray patent portfolio.

72. On information and belief, since at least the above-mentioned date when Defendants were on notice of their infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the ’678 patent to directly infringe one or more claims of the ’678 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the date of notice provided above, Defendants each conduct infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the ’678 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, and other related service providers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States. Moreover, Defendants

manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make available instructions or manuals for these products to consumers, installers, purchasers and prospective buyers, test and certify the wireless networking features (with for example the Wi-Fi Alliance, the Connectivity Standards Alliance, i.e., for ZigBee certification) in the Accused Products, and provide technical support, product files and videos, or related services for these products to purchasers in the United States. *See, e.g.*, *Snap One Support*, SNAP ONE, https://www.snapav.com/shop/en/snapav/support (providing links where consumers may access resources for installing, maintaining, and using Snap One's products) (last visited Nov. 18, 2022).

73. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Snap One's products by designing, developing, marketing, and offering smartphone and tablet interfaces as application software (i.e., apps) to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g.*, *OvrC*, SNAP ONE, https://www.snapav.com/shop/en/snapav/ovrc-connect ("Through the OvrC Connect app, your customers can manage Wi-Fi access and filter network content with the push of a button.") (last visited Nov. 18, 2022); *Get The Most Out Of Your Control4 Smart Home With OS 3*, SNAP ONE, https://www.control4.com/os3/getting-the-most-out-of-os3 (providing a description of Snap One's Control4 which shows users how to "easily navigate and control your smart home effortlessly") (last visited Nov. 18, 2022).

74. Snap One's apps also induce infringing use of the Accused Products by providing compatibility between Snap One products and third-party products that share or access the same

wireless networks. *See, e.g.*, *Complete Smart Home Control Top To Bottom—Inside and Out*, SNAP ONE, https://www.control4.com/solutions/whole-home (stating under the "We Play Nicely with Others" header that "[w]hether you want to use products from other manufacturers or choose the products we have purpose-built for the smart home, it's entirely up to you. Brands like Bose, Dish, Denon, LG, Samsung, and Sony already have Control4 technology built into many of their products, but Control4 also communicates with tens of thousands of devices from over 300 brands.") (last visited Nov. 18, 2022). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants' products, including via the smartphone and tablet Wi-Fi apps and other interfaces utilizing Wi-Fi or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '678 patent. *See 2021 Snap One Annual Report at 8* ("Through our proprietary software, Control4 OS3 and OvrC, we allow integration with thousands of products manufactured by hundreds of third-party manufacturers, and our products are compatible with connected devices from leading brands such as Alphabet, Amazon and Apple, allowing end consumers to enjoy and control their integrated system with the products and devices they know and love.").

75. On information and belief, despite having knowledge of the '678 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '678 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants' infringing activities relative to the '678 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

76. Plaintiff Stingray has been damaged as a result of Defendants' infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for their infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT II

(INFRINGEMENT OF U.S. PATENT NO. 7,440,572)

77. Plaintiff incorporates paragraphs 1 through 76 herein by reference.

78. Plaintiff is the assignee of the '572 patent, entitled "Secure wireless LAN device and associated methods," with ownership of all substantial rights in the '572 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

79. The '572 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '572 patent issued from U.S. Patent Application No. 09/760,619.

80. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '572 patent in this District and elsewhere in Texas and the United States.

81. On information and belief, the Snap One Defendants design, develop, manufacture, import, distribute, offer to sell, sell, and use the Accused Products, including via the activities of Snap Holdings and its subsidiaries, members, segments, companies, brands and/or related entities, such as Defendant Snap LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One.

82. Defendants each directly infringe the '572 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the

fundamental technologies covered by the '572 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendants design the Accused Products for U.S. consumers, make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, installers, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '572 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

83. Furthermore, Defendant Snap Holdings directly infringes the '572 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant Snap LLC, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One, including by designing the Accused Products for U.S. consumers and selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, Snap One's U.S.-based subsidiaries, including at least Snap LLC, conduct activities that constitute direct infringement of the '572 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants, including parent company Snap

Holdings. Defendant Snap Holdings is vicariously liable for the infringing conduct of Defendant Snap LLC and other U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One (under both the alter ego and agency theories). On information and belief, Defendants Snap Holdings, Snap LLC, and other U.S. based subsidiaries members, segments, companies and/or brands of Snap One are essentially the same company (i.e., "Snap One"), operating in the U.S. via at least the Control4™, araknis™, Access Networks®, pakedge®, Clare™, WattBox® SunbriteTV™, and Allnet™ brands, segments, mergers, or acquisitions of Snap One. Moreover, Snap Holdings, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendants each receive a direct financial benefit from that infringement.

84. Defendants infringe claim 1 of the '572 patent via the Accused Products that utilize or are enabled with or compliant with 802.11 (Wi-Fi) protocols, including, but not limited to Defendants' security, smart home, networking, and automation products, such as smart home systems, controllers, touchscreens, wireless keypads, dimmers, remotes, access points, routers, security cameras, power controllers, surge protectors, components, software/firmware, services, processes, related accessories, and mobile applications.

85. Those Accused Products include "[a] secure wireless local area network (LAN) device" comprising the limitations of claim 1. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include a housing; a wireless transceiver carried by said housing; a medium access controller (MAC) carried by said housing; and a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver for encrypting both address and data information for transmission by at least adding a plurality of encrypting bits

to both the address and the data information, and for decrypting both the address and the data information upon reception.

86. At a minimum, Defendants have known of the ’572 patent at least as early as the filing date of this complaint. In addition, Defendants have known about their infringement of L3Harris Corporation’s patent portfolio which Stingray now owns and includes the ’572 patent, since at least its receipt of a letter from Acacia Research Group on behalf of Stingray to Snap One’s predecessor Control4 Corporation, dated July 29, 2020. Stingray also contacted Snap One on April 28, 2021 alleging infringement of patents in the Stingray portfolio, including providing to Defendants Evidence of Use claims charts for portfolio patents and specifically for the ’572 patent. These letters notify Defendants that their products practice at least ZigBee and Wi-Fi wireless network technologies covered by the Stingray patent portfolio.

87. On information and belief, since at least the above-mentioned date when Defendants were on notice of their infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the ’572 patent to directly infringe one or more claims of the ’572 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the date of notice provided above, Defendants each conduct infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the ’572 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users,

and other related service providers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States. Moreover, Defendants manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make available instructions or manuals for these products to consumers, installers, purchasers and prospective buyers, test and certify the wireless networking features (with for example the Wi-Fi Alliance, the Connectivity Standards Alliance, i.e., for ZigBee certification) in the Accused Products, and provide technical support, product files and videos, or related services for these products to purchasers in the United States. *See, e.g.*, *Snap One Support*, SNAP ONE, https://www.snapav.com/shop/en/snapav/support (providing links where consumers may access resources for installing, maintaining, and using Snap One's products) (last visited Nov. 18, 2022).

88. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Snap One's products by designing, developing, marketing, and offering smartphone and tablet interfaces as application software (i.e., apps) to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g.*, *OvrC*, SNAP ONE, https://www.snapav.com/shop/en/snapav/ovrc-connect ("Through the OvrC Connect app, your customers can manage Wi-Fi access and filter network content with the push of a button.") (last visited Nov. 18, 2022); *Get The Most Out Of Your Control4 Smart Home With OS 3*, SNAP ONE, https://www.control4.com/os3/getting-the-most-out-of-os3 (providing a description of Snap One's

Control4 which shows users how to "easily navigate and control your smart home effortlessly") (last visited Nov. 18, 2022).

89. Snap One's apps also induce infringing use of the Accused Products by providing compatibility between Snap One products and third-party products that share or access the same wireless networks. *See, e.g.*, *Complete Smart Home Control Top To Bottom—Inside And Out*, SNAP ONE, https://www.control4.com/solutions/whole-home (stating under the "We Play Nicely with Others" header that "[w]hether you want to use products from other manufacturers or choose the products we have purpose-built for the smart home, it's entirely up to you. Brands like Bose, Dish, Denon, LG, Samsung, and Sony already have Control4 technology built into many of their products, but Control4 also communicates with tens of thousands of devices from over 300 brands.") (last visited Nov. 18, 2022). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants' products, including via the smartphone and tablet Wi-Fi apps and other interfaces utilizing Wi-Fi or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '572 patent. *See 2021 Snap One Annual Report at 8* ("Through our proprietary software, Control4 OS3 and OvrC, we allow integration with thousands of products manufactured by hundreds of third-party manufacturers, and our products are compatible with connected devices from leading brands such as Alphabet, Amazon and Apple, allowing end consumers to enjoy and control their integrated system with the products and devices they know and love.").

90. On information and belief, despite having knowledge of the '572 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '572 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants' infringing activities relative to the '572 patent

have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

91. Plaintiff Stingray has been damaged as a result of Defendants' infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for their infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III

(INFRINGEMENT OF U.S. PATENT NO. 7,441,126)

92. Plaintiff incorporates paragraphs 1 through 91 herein by reference.

93. Plaintiff is the assignee of the '126 patent, entitled "Secure wireless LAN device including tamper resistant feature and associated method," with ownership of all substantial rights in the '126 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements

94. The '126 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '126 patent issued from U.S. Patent Application No. 09/761,173 filed on January 16, 2001.

95. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '126 patent in this District and elsewhere in Texas and the United States.

96. On information and belief, the Snap One Defendants design, develop, manufacture, import, distribute, offer to sell, sell, and use the Accused Products, including via the activities of Snap Holdings and its subsidiaries, members, segments, companies, brands and/or related entities,

such as Defendant Snap LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One.

97. Defendants each directly infringe the '126 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '126 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendants design the Accused Products for U.S. consumers, make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, installers, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '126 patent. *See, e.g.*, *Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

98. Furthermore, Defendant Snap Holdings directly infringes the '126 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant Snap LLC, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One, including by designing the Accused Products for U.S. consumers and selling and offering for sale

the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, Snap One's U.S.-based subsidiaries, including at least Snap LLC, conduct activities that constitute direct infringement of the '126 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants, including parent company Snap Holdings. Defendant Snap Holdings is vicariously liable for the infringing conduct of Defendant Snap LLC and other U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One (under both the alter ego and agency theories). On information and belief, Defendants Snap Holdings, Snap LLC, and other U.S. based subsidiaries members, segments, companies and/or brands of Snap One are essentially the same company (i.e., "Snap One"), operating in the U.S. via at least the Control4™, araknis™, Access Networks®, pakedge®, Clare™, WattBox® SunbriteTV™, and Allnet™ brands, segments, mergers, or acquisitions of Snap One. Moreover, Snap Holdings, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendants each receive a direct financial benefit from that infringement.

99. For example, Defendants infringe claim 1 of the '126 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to Defendants' infringing Accused Products that are enabled or compliant with Wi-Fi and that utilize a battery and a volatile memory for the storage of device data, including cryptographic data. Such Accused Products include, but are not limited to security control panels and keypads (e.g., the ClareOne Wireless Security and Smart Home Panel, model no. CLR-C1-PNL1), Tabletop Touch Screens (e.g., the Control 4 T3-7), and the Neeo Remote for Control4.

100. Those Accused Products include "[a] secure wireless local area network (LAN) device" comprising the limitations of claim 1. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include a housing; a wireless transceiver carried by said housing; a media access controller (MAC) carried by said housing; and a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver, said cryptography circuit comprising at least one volatile memory for storing cryptography information, and a battery for maintaining the cryptography information in said at least one volatile memory.

101. At a minimum, Defendants have known of the '126 patent at least as early as the filing date of this complaint. In addition, Defendants have known about their infringement of L3Harris Corporation's patent portfolio which Stingray now owns and includes the '126 patent, since at least its receipt of a letter from Acacia Research Group on behalf of Stingray to Snap One's predecessor Control4 Corporation, dated July 29, 2020. Stingray also contacted Snap One on April 28, 2021 alleging infringement of patents in the Stingray portfolio. These letters notify Defendants that their products practice at least ZigBee and Wi-Fi wireless network technologies covered by the Stingray patent portfolio.

102. On information and belief, since at least the above-mentioned date when Defendants were on notice of their infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the '126 patent to directly infringe one or more claims of the '126 patent by using, offering for sale, selling, and/or importing the Accused

Products. Since at least the date of notice provided above, Defendants each conduct infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '126 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, and other related service providers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States. Moreover, Defendants manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make available instructions or manuals for these products to consumers, installers, purchasers and prospective buyers, test and certify the wireless networking features (with for example the Wi-Fi Alliance, the Connectivity Standards Alliance, i.e., for ZigBee certification) in the Accused Products, and provide technical support, product files and videos, or related services for these products to purchasers in the United States. *See, e.g.*, *Snap One Support*, SNAP ONE, https://www.snapav.com/shop/en/snapav/support (providing links where consumers may access resources for installing, maintaining, and using Snap One's products) (last visited Nov. 18, 2022).

103. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Snap One's products by designing, developing, marketing, and offering smartphone and tablet interfaces as application software (i.e., apps) to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g.*, *OvrC*, SNAP ONE,

https://www.snapav.com/shop/en/snapav/ovrc-connect ("Through the OvrC Connect app, your customers can manage Wi-Fi access and filter network content with the push of a button.") (last visited Nov. 18, 2022); *Get The Most Out Of Your Control4 Smart Home With OS 3*, SNAP ONE, https://www.control4.com/os3/getting-the-most-out-of-os3 (providing a description of Snap One's Control4 which shows users how to "easily navigate and control your smart home effortlessly") (last visited Nov. 18, 2022).

104. Snap One's apps also induce infringing use of the Accused Products by providing compatibility between Snap One products and third-party products that share or access the same wireless networks. *See, e.g.*, *Complete Smart Home Control Top To Bottom—Inside And Out*, SNAP ONE, https://www.control4.com/solutions/whole-home (stating under the "We Play Nicely with Others" header that "[w]hether you want to use products from other manufacturers or choose the products we have purpose-built for the smart home, it's entirely up to you. Brands like Bose, Dish, Denon, LG, Samsung, and Sony already have Control4 technology built into many of their products, but Control4 also communicates with tens of thousands of devices from over 300 brands.") (last visited Nov. 18, 2022). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants' products, including via the smartphone and tablet Wi-Fi apps and other interfaces utilizing Wi-Fi or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '126 patent. *See 2021 Snap One Annual Report at 8* ("Through our proprietary software, Control4 OS3 and OvrC, we allow integration with thousands of products manufactured by hundreds of third-party manufacturers, and our products are compatible with connected devices from leading brands such as Alphabet, Amazon and Apple, allowing end consumers to enjoy and control their integrated system with the products and devices they know and love.").

105. On information and belief, despite having knowledge of the ’126 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ’126 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants’ infringing activities relative to the ’126 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

106. Plaintiff Stingray has been damaged as a result of Defendants’ infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for their infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT IV

(INFRINGEMENT OF U.S. PATENT NO. 7,616,961)

107. Plaintiff incorporates paragraphs 1 through 106 herein by reference.

108. Plaintiff is the assignee of the ’961 patent, entitled “Allocating channels in a mobile ad hoc network,” with ownership of all substantial rights in the ’961 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

109. The ’961 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The ’961 patent issued from U.S. Patent Application No. 10/134,862.

110. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the ’961 patent in this District and elsewhere in Texas and the United States.

111. On information and belief, the Snap One Defendants design, develop, manufacture, import, distribute, offer to sell, sell, and use the Accused Products, including via the activities of Snap Holdings and its subsidiaries, members, segments, companies, brands and/or related entities, such as Defendant Snap LLC and U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One.

112. Defendants each directly infringe the '961 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '961 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendants design the Accused Products for U.S. consumers, make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, installers, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '961 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

113. Furthermore, Defendant Snap Holdings directly infringes the '961 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant Snap LLC, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One, including by designing the Accused Products for U.S. consumers and selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, Snap One's U.S.-based subsidiaries, including at least Snap LLC, conduct activities that constitute direct infringement of the '961 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants, including parent company Snap Holdings. Defendant Snap Holdings is vicariously liable for the infringing conduct of Defendant Snap LLC and other U.S.-based subsidiaries, members, segments, companies and/or brands of Snap One (under both the alter ego and agency theories). On information and belief, Defendants Snap Holdings, Snap LLC, and other U.S. based subsidiaries members, segments, companies and/or brands of Snap One are essentially the same company (i.e., "Snap One"), operating in the U.S. via at least the Control4™, araknis™, Access Networks®, pakedge®, Clare™, WattBox® SunbriteTV™, and Allnet™ brands, segments, mergers, or acquisitions of Snap One. Moreover, Snap Holdings, as the parent company, along with its related entities, has the right and ability to control and/or delegate such control of the infringing activities of those subsidiary entities such that Defendants each receive a direct financial benefit from that infringement.

114. For example, Defendants infringe claim 1 of the '961 patent via the Accused Products such as at least the Control4® EA-5 Controller, Wireless Configurable Keypad, Wireless Keypad Dimmer, Wireless Thermostat, Fan Speed Controller, and Sensors, which utilize the ZigBee protocol.

115. Those Accused Products include a "method for dynamic channel allocation in a mobile ad hoc network comprising a plurality of wireless mobile nodes and a plurality of wireless communication links connecting the plurality of wireless mobile nodes together over a plurality of separate channels at different frequencies" comprising the limitations of claim 1. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include the steps of at each node, monitoring link performance on a first channel, link performance being based upon at least one quality of service (QoS) threshold; at each node, scouting one or more other available separate channels at different frequencies when the monitored link performance on the first channel falls below the QoS threshold by at least switching to a second separate channel at a different frequency, broadcasting a channel activity query to determine link performance for the second separate channel, and processing replies to the channel activity query to determine the link performance for the second separate channel; and at each node, updating respective channel activity for the first and second separate channels at different frequencies based upon the processed replies.

116. At a minimum, Defendants have known of the '961 patent at least as early as the filing date of this complaint. In addition, Defendants have known about their infringement of L3Harris Corporation's patent portfolio which Stingray now owns and includes the '961 patent, since at least its receipt of a letter from Acacia Research Group on behalf of Stingray to Snap One's predecessor Control4 Corporation, dated July 29, 2020. Stingray also contacted Snap One on April 28, 2021 alleging infringement of patents in the Stingray portfolio, including providing to Defendants Evidence of Use claims charts for portfolio patents and specifically for the '961 patent. These letters notify Defendants that their products practice at least ZigBee and Wi-Fi wireless network technologies covered by the Stingray patent portfolio.

117. On information and belief, since at least the above-mentioned date when Defendants were on notice of their infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the ’961 patent to directly infringe one or more claims of the ’961 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the date of notice provided above, Defendants each conduct infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the ’961 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, and other related service providers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States. Moreover, Defendants manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make available instructions or manuals for these products to consumers, installers, purchasers and prospective buyers, test and certify the wireless networking features (with for example the Wi-Fi Alliance, the Connectivity Standards Alliance, i.e., for ZigBee certification) in the Accused Products, and provide technical support, product files and videos, or related services for these products to purchasers in the United States. *See, e.g.*, *Snap One Support*, SNAP ONE,

https://www.snapav.com/shop/en/snapav/support (providing links where consumers may access resources for installing, maintaining, and using Snap One's products) (last visited Nov. 18, 2022).

118. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Snap One's products by designing, developing, marketing, and offering smartphone and tablet interfaces as application software (i.e., apps) to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g.*, *OvrC*, SNAP ONE, https://www.snapav.com/shop/en/snapav/ovrc-connect ("Through the OvrC Connect app, your customers can manage Wi-Fi access and filter network content with the push of a button.") (last visited Nov. 18, 2022); *Get The Most Out Of Your Control4 Smart Home With OS 3*, SNAP ONE, https://www.control4.com/os3/getting-the-most-out-of-os3 (providing a description of Snap One's Control4 which shows users how to "easily navigate and control your smart home effortlessly") (last visited Nov. 18, 2022).

119. Snap One's apps also induce infringing use of the Accused Products by providing compatibility between Snap One products and third-party products that share or access the same wireless networks. *See, e.g.*, *Complete Smart Home Control Top To Bottom—Inside And Out*, SNAP ONE, https://www.control4.com/solutions/whole-home (stating under the "We Play Nicely with Others" header that "[w]hether you want to use products from other manufacturers or choose the products we have purpose-built for the smart home, it's entirely up to you. Brands like Bose, Dish, Denon, LG, Samsung, and Sony already have Control4 technology built into many of their products, but Control4 also communicates with tens of thousands of devices from over 300 brands.") (last visited Nov. 18, 2022). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants' products, including via the smartphone and tablet Wi-Fi

apps and other interfaces utilizing Wi-Fi or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '961 patent. *See 2021 Snap One Annual Report at 8* ("Through our proprietary software, Control4 OS3 and OvrC, we allow integration with thousands of products manufactured by hundreds of third-party manufacturers, and our products are compatible with connected devices from leading brands such as Alphabet, Amazon and Apple, allowing end consumers to enjoy and control their integrated system with the products and devices they know and love.").

120. On information and belief, despite having knowledge of the '961 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '961 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants' infringing activities relative to the '961 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

121. Plaintiff Stingray has been damaged as a result of Defendants' infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for their infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

CONCLUSION

122. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court.

123. Plaintiff has incurred and will incur attorneys' fees, costs, and expenses in the prosecution of this action. The circumstances of this dispute may give rise to an exceptional case within the meaning of 35 U.S.C. § 285, and Plaintiff is entitled to recover its reasonable and necessary attorneys' fees, costs, and expenses.

JURY DEMAND

124. Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

125. Plaintiff requests that the Court find in its favor and against Defendants, and that the Court grant Plaintiff the following relief:

A. A judgment that Defendants have infringed the Asserted Patents as alleged herein, directly and/or indirectly by way of inducing infringement of such patents;

B. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendants;

C. A judgment and order requiring Defendants to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;

D. A judgment and order requiring Defendants to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;

E. A judgment and order finding this to be an exceptional case and requiring Defendants to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and

F. Such other and further relief as the Court deems just and equitable.

Dated: January 4, 2023

Respectfully submitted,

/s/ Jeffrey R. Bragalone __

Jeffrey R. Bragalone (lead attorney)
Texas Bar No. 02855775
E-mail: jbragalone@bosfirm.com
Terry A. Saad
Texas Bar No. 24066015
E-mail: tsaad@bosfirm.com
Marcus Benavides
Texas Bar No. 24035574
E-mail: mbenavides@bosfirm.com
Brandon V. Zuniga
Texas Bar no. 24088720
E-mail: bzuniga@bosfirm.com
Paul C. Stevenson
Texas Bar No. 24117098
E-mail: pstevenson@bosfirm.com
BRAGALONE OLEJKO SAAD PC
901 Main Street
Suite 3800
Dallas, Texas 75202
Telephone: (214) 785-6670
Facsimile: (214) 785-6680

Wesley Hill
Texas Bar No. 24032294
E-mail: wh@wsfirm.com
WARD, SMITH, & HILL, PLLC
1507 Bill Owens Parkway
Longview, Texas 75604
Telephone: (903) 757-6400
Facsimile: (903) 757-2323

ATTORNEYS FOR PLAINTIFF
STINGRAY IP SOLUTIONS LLC